Maria Raquel Guimarães
Rute Teixeira Pedro
Maria Regina Redinha
(Coordenadoras)

CIJ
CENTRO
DE INVESTIGAÇÃO
JURÍDICA · FDUP

DIREITO DIGITAL 2.0

DIREITO DIGITAL

Maria Raquel Guimarães
Rute Teixeira Pedro
Maria Regina Redinha
(Coordenação)

Fernanda de Araujo Meirelles Magalhães
(Organização)

2023

DIREITO DIGITAL 2.0

COORDENAÇÃO

Maria Raquel Guimarães • Rute Teixeira Pedro • Maria Regina Redinha

[Publicação do Projecto "It's a wonderful (digital) world": O direito numa sociedade digital e tecnológica (CIJ)]

Este trabalho foi desenvolvido com o apoio da Fundação para a Ciência e a Tecnologia – UIDB/00443/2020 (Centro de Investigação Jurídica)

EDIÇÃO

Universidade do Porto • Reitoria

CAPA

Maria Raquel Guimarães

EXECUÇÃO GRÁFICA

Ana Paula Silva

ISBN

978-989-746-362-4

CIJ CENTRO DE INVESTIGAÇÃO JURÍDICA · FDUP

fct Fundação para a Ciência e a Tecnologia

2023

SUMÁRIO

III
OS CONTRATOS SOBRE DADOS

IV
IMPACTO DA TECNOLOGIA E REGULAÇÃO

NOTA DAS COORDENADORAS

Os desenvolvimentos tecnológicos continuam a produzir-se a um ritmo muito acelerado, acentuando a extensão e a velocidade das transformações na vida quotidiana. Não parece existir domínio que permaneça intocado pela revolução digital com que somos confrontados e este fenómeno continua a interpelar o direito.

Quer se considerem os novos produtos dotados de graus crescentes de inteligência artificial, quer se considere o novo meio representado pela internet, os desafios são múltiplos e complexos atentos os movimentos de desterritorialização, desmaterialização e da erosão das barreiras estaduais associados às novas tecnologias. Pense-se, a título ilustrativo, na difusão de informações num *tweet* ou num *post* numa rede social, na contratação *online*, no armazenamento e tratamento de dados em repositórios, bases de dados, nas múltiplas manifestações de "ciência aberta" e de "*cloud computing*", na prática da telemedicina, no recurso a plataformas potenciadoras da denominada economia colaborativa, no uso de assinaturas digitais e *software*, na telematização do trabalho e do processo de tomada de decisões e de formação de deliberações, na desmaterialização do processos civil e penal, nas novas formas de praticar crimes, nomeadamente económicos.

Todos os domínios do direito são convocados para esta reflexão – do direito civil ao direito comercial, do direito do consumidor ao direito empresarial, do direito do trabalho ao direito da propriedade industrial, do direito da propriedade intelectual ao direito penal, dos direitos processuais civil e penal ao direito dos seguros e ao direito fiscal.

Através do projecto "'It's a wonderful (digital) world': O direito numa sociedade digital e tecnológica" procuramos refletir sobre os problemas que esta nova era coloca ao direito e interpelámos, desde logo, os estudantes do Curso de Mestrado em Direito da Faculdade de Direito da Universidade do Porto. Em conjunto, pensámos a proteção dos direitos dos menores na era digital, os contratos sobre dados pessoais, a regulação desses dados e a protecção da privacidade, bem como o impacto da tecnologia e questões de regulação.

Prosseguimos o caminho da publicação das teses de mestrado defendidas com melhor classificação na FDUP no âmbito do Direito Digital. Neste segundo volume publicam-se as que foram defendidas nos anos de 2021 e 2022. Agradecemos a todos os Colegas que integraram os júris nomeados para as provas públicas que apreciaram os trabalhos aqui publicados e, em particular, na qualidade de arguentes, àqueles que sendo externos ao projecto disponibilizaram o seu tempo e saber para a apreciação cuidada dos textos e a interpelação dos candidatos.

É também, mais uma vez, devida uma palavra de reconhecimento à Mestre Fernanda de Araujo Meirelles Magalhães pela organização e revisão cuidadas desta edição.

Aos Autores, endereçamos o nosso agradecimento pelo trabalho entusiasmado e dedicado e felicitamos por este novo feito de "dar a conhecer ao mundo" a sua investigação.

Porto, 4 de Junho de 2023
Maria Raquel Guimarães
Rute Teixeira Pedro
Maria Regina Redinha

I

PROTECÇÃO DOS DIREITOS DOS MENORES NA ERA DIGITAL

A PROTEÇÃO JUSCIVILISTA DAS CRIANÇAS E DOS ADOLESCENTES NA ERA DO *SHARENTING*

Ana Jéssica Romero da Frota Levy

jessicafrota.adv@gmail.com

Resumo: A compreensão da instituição familiar enquanto ambiente de realização e desenvolvimento da personalidade dos seus membros possibilitou o abandono progressivo da concepção paternalista da família e a consequente evolução da imagem social da criança e do adolescente, que passaram a ser percebidos como verdadeiros sujeitos de direitos, dotados de uma autonomia que lhes é própria, condizente com a sua fase da vida e com o seu nível de amadurecimento. Como consequência, o entendimento do direito acerca da relação entre pais e filhos foi remodelado para enxergar no cuidado a noção central a orientar o exercício das responsabilidades parentais. É tomando esse cenário como pano de fundo que os novos desafios jurídicos apresentados pela *Internet* devem ser analisados. Na contemporaneidade, um problema que vem se apresentando aos juristas diz respeito ao compartilhamento pelos pais de informações pessoais dos filhos menores de idade nas redes sociais. Apelidado de *sharenting*, esse fenômeno coloca em tensão a liberdade de expressão dos pais e o seu *status* como guardiões primeiros dos filhos e a tutela dos direitos de personalidade da criança, nomeadamente a salvaguarda do seu direito à privacidade. Esta tese se propõe a examinar essa factualidade, própria da era digital, a partir da ótica personalista da família, investigando os mecanismos legais de reação possíveis em caso de graves ofensas à personalidade das crianças e dos adolescentes.

Palavras-chave: *sharenting*; incapacidade por menoridade; superior interesse da criança; responsabilidades parentais; cuidado parental; direitos de personalidade; direito à privacidade; responsabilidade civil dos progenitores; direito ao esquecimento.

Abstract: The understanding of the family institution as an environment for the realization and development of the personality of its members made it possible to progressively abandon the paternalistic conception of the family and the consequent evolution of the social image of children and adolescents, who came to be perceived as true subjects of rights, endowed with a particular autonomy, consistent with their life stage and with their level of maturity. As a result, the legal understanding of the relationship between parents and their children was remodeled to see care as the central notion relating to the exercise of parental responsibilities. It is against this backdrop that the new legal challenges presented by the *Internet* must be analyzed. In contemporary times, a problem that has been presenting itself to jurists concerns the sharing by parents of their underage children's personal information on social networks. Called *sharenting*, this phenomenon puts into tension the parents' freedom of expression and their *status* as the first guardians of their children and the protection of the child's personality rights, namely the safeguarding of their right to privacy. This thesis proposes to examine this factuality, typical of the digital age, from the personalist perspective of the family, investigating the legal reaction mechanisms possible in case of serious offenses to the personality of children and adolescents.

Keywords: *sharenting*; legal incapacity of minors; best interests of the child; parental responsibilities; parental care; personality rights; right to privacy; parental civil liability; right to be forgotten.

1. INTRODUÇÃO

Considere-se a situação que passamos a expor. Com 14 anos de idade, Maria está sendo vítima de piadas na escola em razão de fotos compartilhadas por seus pais no *Facebook* de quando ainda era bebê. Apesar de, tempos antes, Maria ter manifestado sua insatisfação com as publicações, seus pais se recusaram a retirar as fotografias das redes sociais. Segundo afirmou sua mãe, as postagens aconteceram em contas privadas do *Facebook*, que só poderiam ser acessadas por amigos e familiares, não havendo motivo para preocupações. Mais severo, seu pai declarou que tinha o direito de postar o que quisesse em sua própria conta, como resultado da sua liberdade de expressão.

Conquanto hipotética, a situação narrada acima revela um cenário que tem se tornado cada vez mais comum no seio das famílias diante do avanço das tecnologias e das mídias sociais. Trata-se de um fenômeno apelidado de *sharenting* – termo utilizado para se referir ao compartilhamento de informações pessoais dos filhos pelos pais na *Internet*. Esta tese se propõe a analisar juridicamente esse fenômeno, considerando as repercussões que ele ocasiona na esfera de personalidade das crianças e dos adolescentes e os mecanismos de reação às consequências desvantajosas.

Para isso, no primeiro capítulo, será explorada a evolução da imagem social do sujeito menor de idade associada à reconfiguração da família como ambiente de realização pessoal dos seus membros. Analisar-se-á o reconhecimento da criança e do adolescente como verdadeiros sujeitos de direitos, providos de uma autonomia que se faz sentir de modo diverso em razão da sua fase de desenvolvimento e na medida de sua maturidade.

A identificação do jovem como pessoa dotada de gradual capacidade gerou, como não poderia deixar de ser, repercussões na maneira como o direito se propõe a balizar o relacionamento entre pais e filhos. Nesse sentido, o segundo capítulo do presente estudo delineará as bases legais do exercício das responsabilidades parentais, investigando-se a íntima relação entre os poderes-deveres a ela associados e o desenvolvimento da personalidade dos filhos.

O terceiro capítulo examinará de que modo as bases até então apresentadas se aplicam em face dos novos desafios propostos pelo mundo digital, especificamente em casos nos quais a partilha de imagens e vídeos dos filhos pelos pais nas redes sociais comportam riscos copiosos à privacidade e à imagem da criança.

Por fim, no último capítulo, será averiguado o arcabouço jurídico-normativo português em busca de respostas que possam, adequadamente, salvaguardar os direitos de personalidade dos filhos menores de idade quando os progenitores excedam à sua esfera de liberdade através da prática imoderada de *sharenting*.

2. A CRIANÇA E O ADOLESCENTE COMO SUJEITOS DE DIREITOS

2.1. A EVOLUÇÃO HISTÓRICA DA PERSPECTIVAÇÃO JURÍDICA DA PESSOA COM IDADE INFERIOR A 18 ANOS: DA SUA CONCEPÇÃO COMO MENOR À SUA CONCEPÇÃO COMO "CRIANÇA E JOVEM"

A concepção da criança e do jovem como sujeitos de direitos, cuja autonomia (como centro de interesses próprios e como ser dotado de capacidade, apesar da vulnerabilidade resultante da idade) deve ser reconhecida e promovida, constitui, entre nós, aquisição recente, resultado de um movimento paulatino de valorização da sua qualidade de pessoa. Essa evolução da sua situação jurídica acompanha o valor que a sociedade de determinado momento histórico atribui à infância e o alcance da intervenção do Estado sobre a família, como meio de controle da autoridade paternal[1].

Na Idade Média, por exemplo, é custoso se vislumbrar uma consciência social acerca da infância enquanto realidade específica[2/3]. O alto índice de mortalidade da época obstava um investimento afetivo a nível social que impulsionasse o reconhecimento da pessoa da criança[4]. A criança era vista como um "adulto em miniatura", diferenciando-se apenas em relação ao tamanho e a força para o trabalho, sem lugar para a identificação das etapas da infância ou da juventude[5].

---

1 Cristina Dias, "A criança como sujeito de direitos e o poder de correcção" *in Revista JULGAR*, n.º 4, 2008, cit., p. 98, disponível em http://julgar.pt/a-crianca-como-sujeito-de-direitos-e-o-poder-de-correccao/ (20/09/2021).

2 Rosa Cândido Martins, "Responsabilidades parentais no século XXI: a tensão entre o direito de participação da criança e a função educativa dos pais" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 5, n.º 10, Coimbra Editora, 2008, cit., p. 27.

3 A arte medieval serve de espelho dessa realidade. Como chama atenção Guilherme de Oliveira, "até os pintores, quando figuravam crianças, desenhavam corpos pequenos com cara de adultos", *vide* GUILHERME DE OLIVEIRA, "A criança maltratada" *in Interacções – Revista do Instituto Superior de Serviço Social de Coimbra*, n.º 1, 1995, cit., p. 55.

4 "Ninguém pensava em conservar o retrato de uma criança que tivesse sobrevivido e se tornado adulta ou que tivesse morrido pequena. No primeiro caso, a infância era apenas uma fase sem importância, que não fazia sentido fixar na lembrança; no segundo, o da criança morta, não se considerava que essa coisinha desaparecida tão cedo fosse digna de lembrança [...] As pessoas não se podiam apegar muito a algo que era considerado uma perda eventual." Cf. Philippe Ariès, *História social da criança e da família*, 2ª ed, Rio de Janeiro, Guanabara Koogan S.A, 1978, cit., p. 56-57.

5 "A duração da infância era reduzida a seu período mais frágil, enquanto o filhote do homem ainda não conseguia bastar-se; a criança então, mal adquiria algum desembaraço físico, era logo misturada aos adultos, e partilhava de seus trabalhos e jogos. De criancinha pequena, ela se transformava imediatamente em homem jovem, sem passar pelas etapas da juventude." Cf. Philippe Ariès, *História social...*, cit., p. 10.

Os sinais de afirmação de um sentimento da infância tornaram-se mais significativos a partir do fim do século XVI e durante o século XVII[6], com a paralela evolução da instituição escolar, designadamente com a organização do colégio em classes de acordo com a idade[7]. Ainda que timidamente, a família reduzia sua autoridade frente à autoridade das escolas e, de maneira pariforme, crescia o controle do Estado sobre o modo como os pais exerciam essa autoridade[8].

Com a Revolução Industrial e a exploração recorrente do trabalho infantil nas fábricas, despertou-se uma consciência coletiva que pugnava pela intervenção protecionista do Estado em favor da infância[9].

Nesse contexto, na segunda metade do século XIX, pôde-se assistir à produção de leis que se destinavam a limitar o mau exercício da autoridade na família[10], revelando "uma intromissão clara e firme do Estado numa esfera social que lhe estivera vedada até aí"[11].

Apelidado por Ellen Key de "o século da criança"[12], foi no século XX, todavia, que o movimento de reconhecimento dos direitos da criança encontrou maior força de expressão[13]. Durante seu decorrer, o prisma sob a qual a criança era encarada pela sociedade e pelo direito foi substancialmente alterado: de objeto de proteção do Estado ascendeu à categoria de sujeito de direito[14]. Sobre esta nova concepção, vamos versar nas próximas subsecções.

a) A pessoa menor de idade como objeto de tutela estatal

A primeira metade do século XX seguiu marcada pelo sistema patriarcal de sociedade que permeou os séculos anteriores, no qual a posição jurídica

---

6 A infância continuou a ser encarada, entretanto, sob um enfoque negativo. Na realidade, a consciência das particularidades da criança e a sua consequente separação do mundo dos adultos significaram, nesse instante, tão somente uma consciência da sua incapacidade. Cf. Rosa Cândido Martins, *Responsabilidades parentais...*, cit., p. 28.

7 Philippe Ariès, *História social...*, cit., p. 169 e ss.; Maria Clara Sottomayor, "O poder paternal como cuidado parental e os direitos da criança" *in Cuidar da Justiça de Crianças e Jovens: a função dos Juízes Sociais*, Maria Clara Sottomayor [ET AL], Coimbra, Almedina, 2003, cit., p. 11.

8 Guilherme De Oliveira, *A criança...*, cit., p. 56.

9 Rosa Cândido Martins, *Responsabilidades parentais...*, cit., p. 29.

10 Em Portugal, o Código Civil de 1867 dispunha (art. 141) que os pais poderiam ser punidos no caso de abuso no exercício do (então denominado) poder paternal, enquanto o Código Penal de 1886 previa o crime de "exposição" e de "abandono de infantes" (art. 345 a 348).

11 Guilherme De Oliveira, *A criança...*, cit., p. 56.

12 No ano de 1900, a escritora sueca Ellen Key publicou livro intitulado "O Século da Criança" (*Barnets århundrade*), defendendo o desenvolvimento e o bem-estar das crianças como interesses da maior importância para a sociedade.

13 Armando Leandro, "Protecção dos direitos das crianças em Portugal" *in Direitos das Crianças*, A. Reis Monteiro [Et Al], Coimbra, Coimbra Editora, 2004, cit., p. 102.

14 Rosa Cândido Martins, *Responsabilidades parentais...*, cit., p. 30.

de cada membro familiar era perspectivada a partir do "papel que cada um era chamado a desempenhar no seio da família"[15].

A essa estrutura hierarquizada da família se associava à concepção de que a autoridade parental exprimia um verdadeiro poder de domínio do pai, enquanto "chefe de família", em relação aos filhos[16].

Perceber a posição que a criança assumia no âmbito da família patriarcal viabiliza a compreensão da resposta dada pelo direito num primeiro momento de busca pela proteção da pessoa menor de idade. De fato, a visão da criança como ser frágil e incapaz do ponto de vista físico, intelectual e relacional fazia dela "objeto" da proteção estatal também na seara jurídica[17].

É nesse contexto que se insere a Declaração dos Direitos da Criança de 1924, adotada pela dissolvida Sociedade das Nações. Apesar de ter o mérito de ser a primeira a utilizar a expressão "direitos das crianças", a Declaração não chegou a elencar quaisquer direitos, apenas refletindo a suposição então assente de que as crianças poderiam e deveriam contar com a proteção dos adultos na satisfação de suas necessidades econômicas, sociais e psicológicas. Suposição esta que persistiu e, igualmente, permeou a Declaração Universal dos Direitos da Criança, adotada pela Assembleia Geral das Nações Unidas em 1959[18].

Em Portugal, a afirmação da intervenção protetora do Estado se deu logo após a implantação da Primeira República, através da Lei de Protecção à Infância (LPI), de 27 de maio de 1911. Foram com este diploma introduzidas as bases de um sistema de tutela[19], cujas linhas reitoras eram "proteger, regenerar, tornar útil"[20].

---

15 Rute Teixeira Pedro, "A visão personalista da família e a afirmação de direitos individuais no seio do grupo familiar: a emergência de um novo paradigma decorrente do processo de constitucionalização do direito da família" *in Pessoa, Direito e Direitos: Colóquio 2014/2015*, Braga, Universidade do Minho, 2016, cit., p. 338.

16 Maria Clara Sottomayor, *O poder paternal*..., cit., p. 11.

17 Rosa Cândido Martins, *Responsabilidades parentais*..., cit., p. 31.

18 Geraldine Van Bueren, *International Documents on Children*, Second edition, Kluwer Law International, 1998, cit., p. 15.

19 Aprovada com a publicação dos Decretos-Lei n.º 44.287 e 44.288 de 20 de abril de 1962, a Organização Tutelar de Menores (OTM) promoveu alterações profundas no regime inaugurado pela LPI, mantendo, sem embargo, sua lógica intervencionista e protecionista; lógica que permeou, igualmente, a versão da OTM de 1978. Cf. Rui Assis, "A reforma do direito dos menores: do modelo de proteção ao modelo educativo" *in Cuidar da Justiça de Crianças e Jovens: a função dos Juízes Sociais*, Maria Clara Sottomayor [Et Al], Coimbra, Almedina, 2003, cit., p. 138.

20 S/A, *Edição Comemorativa da Lei de Protecção da Infância, 27 de Maio de 1911*; coord. Carlos Poiares, Lisboa, Instituto da Segurança Social, 2010, disponível em https://www.cnpdpcj.gov.pt/documents/10182/14804Edi%C3%A7%C3%A3o+Comemorativa+da+Lei+de+Prote%C3%A7%C3%A3o+da+Inf%C3%A2ncia/f4726737-b519-4d49-a7f-3-59ab3eda4cae (01.06.2022), cit., p.11.

A discursividade legislativa portuguesa admitiu a pessoa menor de idade como ser dotado de peculiaridades que o distinguem do adulto, procedendo, por isso, "a uma profunda reformulação dos órgãos judiciários a quem era confiada a aplicação de medidas aos menores, sobretudo através da criação das chamadas 'tutorias de infância'"[21]. No entanto, não diferente do tom assumido no cenário internacional, a cognição das particularidades da infância pelo legislador nacional se limitou a enxergar a criança como ser débil e incapaz, circunstância que legitimava, *per se*, a ingerência do Estado[22]. Esta perspectivação tem reflexo, como se verá, no ordenamento jurídico português atual, nomeadamente na sua Constituição e também em múltiplos diplomas que dão concretização à proteção da criança e jovem.

b) a criança e o jovem como sujeitos de direitos, enquanto pessoas de indeclinável dignidade

A diversificação das formações familiares no plano fático ao longo do século XX[23] contribuiu para fazer caducar o sistema patriarcal de sociedade e de família que havia imperado nos séculos anteriores.

A nova realidade impulsionou uma releitura da família, que passou a ser encarada como "espaço de exercício de liberdade e de afirmação e concretização de direitos dos seus membros – sejam fundamentais, sejam direitos de personalidade"[24].

Em paralelo a essa tendência, a imagem social da criança deixou de ser esgotada na sua fragilidade para abranger a sua concepção como pessoa dotada de sentimentos e vontades[25], o que acabou por culminar na consa-

---

21 Rui Assis, *A reforma do direito...*, cit., p. 138.

22 Trecho do texto do Ministério da Justiça que antepõe a LPI reflete bem esse sentimento, *i.l.*: "A criança, deixada ao acaso de si mesma ou entregue a pais, tutores e detentores que, longe de lhe reprimir os instintos naturais, afeiçoando-as às necessidades duma vida honesta, as deformam em proveito dos seus próprios vícios, as descuram por perversão, desleixo ou incapacidade educativa; a criança, exposta à mendicidade, à vadiagem, à malvadez, à especulação, à gatunice, à prostituição, arrastada por todas as correntes de corrupção, numa idade em que, por debilidade, por imprevidência, não pode ter o menor movimento de reacção contra essa corrente; a criança, alheia aos mais rudimentares estímulos de perfeição moral, estranha às branduras do amor e da bondade, desconhecendo o espírito de abnegação e de sacrifício, será apenas, e lamentávelmente, um factor permanente de vício, da maldade, da perversão em todas as suas manifestações desorganizadoras". Cf. S/A, *Edição comemorativa...*, cit., p. 11-12.

23 Rute Teixeira Pedro aponta como tendências desse movimento transformador a dissociação entre filiação e casamento, a redução do número de casamentos, a multiplicação das ruturas matrimoniais e o aumento das uniões não matrimonializadas. Cf. Rute Teixeira Pedro, *A visão personalista...*, cit., p. 341.

24 Rute Teixeira Pedro, *A visão personalista...*, cit., p. 348.

25 "As concepções mais recentes da infância recusam-se a defini-la como imaturidade e dependência. Uma criança não é uma pessoa adulta incompleta, mas uma pessoa com experiências diferentes das dos adultos, mas nem mais nem menos coerentes do que

gração de uma "nova cultura jurídica"[26] no que diz respeito à situação das pessoas menores de idade[27].

A criança e o adolescente passam a ser vistos não mais como meros sujeitos passivos, "objetos" das decisões de outrem e carentes da proteção do Estado, mas como verdadeiros sujeitos de direitos, "dotados de uma progressiva autonomia no exercício dos seus direitos em função da sua idade, maturidade e desenvolvimentos das suas capacidades"[28].

Marco fundamental dessa novel consciência jurídica, a Convenção sobre os Direitos da Criança (CDC) de 1989[29] estabelece um sistema de proteção integrada da criança, que a enxerga como ser humano de indelével dignidade e, como tal, sujeito de direitos. Para mais, distintamente de suas predecessoras revestidas de mera eficácia moral, a CDC tem força vinculante à medida que é ratificada, impondo aos Estados Partes o dever jurídico de adequar o seu direito interno às normas da Convenção[30].

Dentre os princípios fundamentais que subjazem à CDC, quatro são os seus alicerces: o princípio de que é dever dos Estados Partes garantir que as crianças sob sua jurisdição gozem dos direitos previstos na Convenção, sem discriminação e independentemente de qualquer consideração relativa à sua incapacidade (art. 2.º); o princípio do "superior interesse da criança", segundo o qual todas as decisões que digam respeito à criança devem ter em conta o seu interesse superior (art. 3.º); o princípio de que todas as crianças têm os direitos à vida, à sobrevivência e ao desenvolvimento (art. 6.º); e o princípio do respeito pelas opiniões da criança, que deve ser livre para exprimi-las e que tem o direito de vê-las tomadas em consideração, de acordo com sua idade e maturidade, em questões que lhe digam respeito (art. 12.º)[31].

---

as destes." Cf. Maria Clara Sottomayor, "Liberdade de opção da criança ou poder do progenitor? – comentário ao Acórdão do Tribunal da Relação de Coimbra, de 31 de outubro de 2007" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 5, n.º 9, Coimbra Editora, jan./jun. 2008, cit., p. 59.

[26] Para utilizar a expressão adotada por Rui Assis. Cf. Rui Assis, *A reforma do direito...*, cit., p. 144.

[27] Nessa perspectiva, por sua conotação de inferioridade, a expressão "menor" não se mostra idônea para traduzir a dignidade da pessoa menor de idade, motivo pelo qual se percebe seu progressivo abandono pela doutrina.

[28] Rosa Cândido Martins, "Poder paternal vs. autonomia da criança e do adolescente" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 1, n.º 1, Coimbra Editora, 2004, cit., p. 69; Em igual sentido, Rui Assis, *A reforma do direito...*, cit., p. 145.

[29] A CDC foi adotada pela Assembleia Geral da ONU em 20 de novembro de 1989 e ratificada por Portugal em 21 de setembro de 1990. É o instrumento de direitos humanos mais aceito na história universal, tendo sido ratificado por 196 países.

[30] Rosa Cândido Martins, *Responsabilidades parentais...*, cit., p. 32-33.

[31] Catarina Albuquerque, "Os Direitos da Criança em Portugal e no Mundo Globalizado: o princípio do interesse superior da criança" *in Direitos das Crianças*, A. Reis Monteiro [ET AL], Coimbra, Coimbra Editora, 2004, cit., p. 40-41.

Entre nós, a visão personalista da família encontrou guarida na Constituição de 1976 (CRP), como decorrência dos princípios base da República Portuguesa, designadamente do princípio angular da dignidade da pessoa humana (art. 1.º) e do "respeito" e "garantia de efetivação dos direitos e liberdades fundamentais" (art. 2.º). A esse propósito, avulta a identificação, pelo art. 67.º, da importância da família para "a realização pessoal dos seus membros"[32].

A axiologia constitucional reverberou a nível infraconstitucional, compelindo a reformulação legislativa do direito de família, cujo vértice pode ser compreendido a partir das transformações operadas pelo Decreto-lei n.º 496/77 ao Código Civil (CC), de onde seguiu-se a compreensão de que a personalidade da criança e dos jovens, com as especificidades que apresenta, deve ser salvaguardada também no íntimo do núcleo familiar[33].

2.2. A (IN)CAPACIDADE POR MENORIDADE

O reconhecimento do estatuto de pessoa às crianças e aos jovens não implicou, nem poderia implicar, no estabelecimento de uma total paridade com o tratamento normativo dispensado aos adultos.

Nesse sentido, consoante o art. 123.º, do CC, as pessoas que ainda não completaram dezoito anos de idade[34], carecem, em princípio, de capacidade para o exercício de direitos. A correta compreensão desse preceito exige que seja feita uma breve explanação acerca dos conceitos de personalidade, de capacidade de gozo e de capacidade de exercício.

Na formulação de Orlando de Carvalho, "a personalidade jurídica é a projecção no Direito (no mundo do normativo jurídico) da personalidade humana"[35], e "implica a susceptibilidade abstracta de ser titular de direitos e de

---

[32] Jorge Miranda; Rui Medeiros, *Constituição Portuguesa anotada. Tomo I: Introdução geral, preâmbulo, artigos 1º a 79º*; colab. Maria da Glória Garcia [et. al.], 2ª ed., Coimbra, Wolters Kluwer Portugal, 2010, cit., p. 807.

[33] "O Código Civil, na versão de 1977 que hoje vigora, é ainda mais subtil na proteção das crianças e dos jovens. Na verdade, a nossa lei não se limita a estabelecer os limites ao exercício da autoridade, ou as condições em que esse exercício passa a ser considerado abusivo. Não se limita a prever o que ilícito aos pais. Mais do que isto, impõe aos pais um dever positivo de respeito pela personalidade dos filhos." Cf. Guilherme De Oliveira, *A criança...*, cit., p. 57.

[34] Rosa Martins extrai o conceito de "menoridade" da conjugação dos dispositivos do Código Civil que regulam a incapacidade por menoridade (art. 122.º a 129.º, CC). Segundo a autora, "é possível afirmar que, do ponto de vista do direito civil, a menoridade consiste no lapso de tempo da vida humana que começa no dia do nascimento (completo e com vida) de um dado sujeito e termina no dia em que este completar o décimo oitavo ano de vida. Tal lapso de tempo corresponde à duração do estado (civil) de menor", *vide* Rosa Martins, *Menoridade, (In)capacidade e Cuidado Parental*, Coimbra: Coimbra Editora, 2008, cit., p. 16.

[35] Orlando De Carvalho, *Teoria Geral do Direito Civil*, coordenação de Francisco Liberal Fernandes, Maria Raquel Guimarães, Maria Regina Redinha, 3ª ed., Coimbra, Coimbra Editora, 2012, cit., p. 190.

deveres"[36]. Enquanto qualidade ou condição jurídica, a personalidade não admite limitações, e "todas as pessoas singulares, desde que nascem até que morrem, a têm, como expressão do seu fundamental valor humano"[37].

Inerente à personalidade e dela indissociável, a capacidade jurídica (ou capacidade de gozo de direitos) é a susceptibilidade concreta de ser titular de direitos e obrigações[38], referindo-se à "aptidão para ser titular de um círculo, maior ou menor, de relações jurídicas"[39].

Apesar de tendencialmente coincidentes, as duas noções não se confundem. Se a personalidade é um *quale*, a capacidade é um *quantum*[40/41], comportando restrições em determinadas condições ou situações. É dizer: a capacidade de determinada pessoa pode ser mais ou menos ampla[42].

A capacidade de exercício (ou capacidade de agir) se traduz, por seu turno, na idoneidade para atuar juridicamente de maneira pessoal, livre e autônoma, seja por ato próprio seja mediante um representante voluntário ou procurador[43]. Está, assim, intimamente ligada à "capacidade natural para querer e entender"[44].

Como se deixou antever, os sujeitos menores de idade estão feridos de uma incapacidade geral de agir (art. 123.º, CC). É dessa incapacidade que nos ocuparemos nos tópicos a seguir[45].

---

36 Orlando De Carvalho, *Teoria Geral...*, cit., p. 259.

37 Raul Guichard, "Sobre a Incapacidade dos Menores no Direito Civil e a sua Justificação" *in Review of Business and Legal Sciences/Revista de Ciências Empresariais e Jurídicas*, n.º 6, pp. 103-148, 2005, disponível em https://doi.org/10.26537/rebules.v0i6.813 (20.09.2021), cit., p. 119.

38 Orlando De Carvalho, *Teoria Geral...*, cit., p. 259.

39 Carlos Alberto Da Mota Pinto; António Pinto Monteiro; Paulo Mota Pinto, *Teoria geral do direito civil*, Coimbra, Coimbra Editora, 5.ª ed., 2020, cit., p. 220.

40 Orlando De Carvalho, *Teoria Geral...*, cit., p. 259.

41 "Ou há uma pessoa jurídica ou não há. Há uma capacidade jurídica maior ou menor". Cf. Carlos Alberto Da Mota Pinto; António Pinto Monteiro; Paulo Mota Pinto, *Teoria geral...*, cit., p. 220.

42 A ressalva contida no art. 67.º do CC ("salvo disposição em contrário") traduz essa possibilidade.

43 Carlos Alberto Da Mota Pinto; António Pinto Monteiro; Paulo Mota Pinto, *Teoria geral...*, cit., p. 221.

44 Rosa Martins, *Menoridade, (In)capacidade...*, cit., p. 51. Ainda, nas palavras de Raul Guichard, "deve acentuar-se o incindível nexo entre a autonomia (privada), como possibilidade de conformação das relações jurídicas por livre vontade dos particulares, e a capacidade (de exercício). Não tem sentido falar em autonomia, não estando a pessoa em causa, *a priori*, em condições de entender completamente a relevância dos seus actos, de reconhecer correctamente os seus interesses, valorá-los e escolher os meios adequados à sua satisfação", *vide* Raul Guichard, *Sobre a Incapacidade...*, cit., p. 131.

45 Como pessoas que são, as pessoas menores gozam, em regra, de capacidade jurídica. Podem, todavia, ser afetadas por incapacidades de gozo em determinadas hipóteses. É o que acontece com as previsões dos artigos 1601.º (falta de capacidade para casar do menor de dezesseis anos), 1850.º (falta de capacidade para perfilhar antes dos dezesseis anos) e 2189.º (incapacidade para testar dos "menores não emancipados"), todos do CC;

Antes, contudo, uma última observação é digna de nota. Não se há confundir a menoridade com a incapacidade de agir por menoridade. Com efeito, o "estado de menor" não corresponde impreterivelmente a uma situação de incapacidade. É possível que um sujeito apesar de não ter ainda completado os dezoito anos de vida seja dotado de capacidade de agir: é o caso do "menor emancipado pelo casamento" (arts. 132.º, 133.º, 1600.º e 1601.º, a, CC)[46].

a) O modelo anterior da incapacidade genérica

Ao atribuir à incapacidade de exercício por menoridade um caráter genérico, a lei estabelece, de acordo com o entendimento tradicional, uma proibição de os sujeitos menores de idade praticarem qualquer ato jurídico de natureza patrimonial ou pessoal[47], sob pena de anulabilidade (art. 125.º, CC). Destarte, os atos praticados pessoalmente pelo sujeito menor no âmbito de sua incapacidade são eivados de invalidade[48].

Tal perspectiva encontra fundamento na clássica concepção da criança e do adolescente como "seres humanos especialmente diminuídos"[49], cujos níveis de maturidade e de esclarecimento os colocam em uma situação de inferioridade. Daí que "a justificação corrente desta incapacidade para agir, universalmente reconhecida, está na necessidade de defender os menores contra as suas próprias fraquezas"[50].

À vista disso, a participação dos sujeitos menores de idade no tráfico jurídico se dá através do instituto da representação, que cabe, em regra, aos pais e, subsidiariamente, a um tutor ou administrador de bens (art. 124.º c/c 1922.º, CC). A capacidade de agir desses sujeitos é exercitada, por conseguinte, pelo representante legal que age em substituição do incapaz no exercício dos seus direitos e no cumprimento de suas obrigações[51].

---

vide Pedro Pais De Vasconcelos; Pedro Leitão Pais De Vasconcelos, *Teoria Geral de Direito Civil*, 9.ª. ed., Coimbra, Almedina, 2019, cit., p. 118-119. Rosa Martins se distancia do entendimento ora esposado ao considerar que as referidas incapacidades são, em verdade, casos de incapacidade de agir insupríveis, por se tratar de atuações personalíssimas, *vide* ROSA MARTINS, *Menoridade, (In)capacidade...*, cit., p. 82 e ss.

46 Assim como quando atingida a maioridade, a emancipação faz cessar a incapacidade por menoridade (art. 129.º, CC). Nesse sentido, Pedro Pais De Vasconcelos; Pedro Leitão Pais De Vasconcelos, *Teoria Geral...*, cit., p. 120. Todavia, essa equiparação de efeitos não faz do "menor emancipado" "maior". Em razão disso, quando nos referirmos ao sujeito menor de idade, à criança ou ao adolescente deve-se inferir que se está a tratar de pessoas menores de dezoito anos não emancipadas.

47 Carlos Alberto Da Mota Pinto; António Pinto Monteiro; Paulo Mota Pinto, *Teoria geral...*, cit., p. 228; ROSA MARTINS, *Menoridade, (In)capacidade...*, cit., p. 91.

48 Pedro Pais De Vasconcelos; Pedro Leitão Pais De Vasconcelos, *Teoria Geral...*, cit., p. 121.

49 Rosa Martins, *Menoridade, (In)capacidade...*, cit., p. 90.

50 Guilherme De Oliveira, "Protecção de menores/Protecção familiar" *in Temas de Direito da Família, 1*, Coimbra, Coimbra Editora, 1999, cit., p. 268.

51 Rosa Martins, *Menoridade, (In)capacidade...*, cit., p. 51.

Malgrado a visão tradicional acerca da incapacidade em razão da idade seja determinada a partir do interesse do próprio incapaz, é certo que o conteúdo daquilo que se entende por esse interesse é substancialmente diferente de outrora. Deveras, diante da perspectivação da criança e do jovem como sujeitos de direitos, deixou de ser concebível que "é do 'interesse da criança' ser tratada como um ser totalmente incapaz de pensar, de decidir e de querer"[52]. E, isso se dá porque a autonomia intrínseca à personalidade do sujeito requer que ele só fique impedido de movimentar a sua esfera jurídica por ato próprio até a medida em que não seja naturalmente capaz de se determinar autonomamente, segundo critérios de necessidade e proporcionalidade[53].

b) O modelo mais recente de reconhecimento gradual de capacidade

O tratamento monolítico da menoridade não se mostra em consonância com a visão contemporânea da criança, cujo grau de maturidade é alcançado de maneira progressiva a partir das suas distintas fases de crescimento[54]. Bem por isso, conforme aponta Maria Clara Sottomayor, "as mais recentes reformas dos códigos civis na Europa orientam-se por um princípio geral de capacidade natural dos menores, de acordo com as faculdades físicas, intelectuais e volitivas presentes em cada fase ou etapa de desenvolvimento"[55].

Impelidos pela lógica gradualista, alguns ordenamentos jurídicos contaram com a previsão de diferentes "estádios etários", em um genuíno "escalonamento etário do regime da menoridade"[56/57]. Não foi essa, entretanto, a opção do legislador português.

---

52 Rui Assis, *A reforma do direito...*, cit., p. 144.

53 Mafalda Miranda Barbosa, "Breves reflexões em torno do art. 127.º do Código Civil" *in Boletim da Faculdade de Direito – Universidade de Coimbra*, Vol. XC, Tomo II, Coimbra, 2014, cit., p. 695.

54 "O menor de cinco anos tem um grau de autonomia e maturidade diverso do menor de dez anos e, ainda mais, do jovem adulto com dezessete anos. Ora, o direito – que não se queira pautar pelo puro formalismo e conceptualismo – não pode deixar de ter em consideração esta realidade à qual se vai aplicar". Cf. Mafalda Miranda Barbosa, *Breves reflexões...*, cit., p. 695.

55 Maria Clara Sottomayor, "Interesse da criança e ética do cuidado" *in Publicações ELSA Coimbra*, 1 de junho de 2021, disponível em https://clarasottomayor.com/public/files/interessecrianca.pdf (24.06.2021), cit., p. 2.

56 Mafalda Miranda Barbosa, *Breves reflexões...*, cit., p. 697.

57 A doutrina aponta a experiência alemã e a experiência austríaca. Tanto o *Bürgeliches Gesetzbuch* (BGB) como o *Allgemeinem bürgerlichen Gesetzbuch* (ABGB) reconhecem a existência de escalões ou patamares de menoridade, aos quais se aplicam regimes jurídicos diferenciados. Resulta do direito alemão, a definição de dois escalões de menoridade: os sujeitos com menos de sete anos e os sujeitos maiores de sete, mas menores de dezoito anos. Por sua vez, do direito austríaco extraem-se três patamares etários: o primeiro patamar compreende as crianças com menos de sete anos; o segundo, as crianças entre sete e catorze anos; o terceiro, as crianças entre catorze e dezoito anos. A esse respeito, *vide* Raul Guichard, *Sobre a Incapacidade...*, cit., p. 115-117, nota n.º 5; Rosa Martins,

Como se depreende do art. 122.º do CC, o sistema de passagem da menoridade à maioridade na ordem jurídica de Portugal se dá através da fixação de um limite etário, qual seja os dezoito anos de idade. Nada obstante, é certo que o quadro do regime jurídico português da menoridade não é indiferente à exigência de autonomização gradual da criança e do adolescente[58].

A primeira questão que se impõe diz respeito à dicotomia entre o exercício dos direitos da personalidade e a submissão dos sujeitos menores ao regime da incapacidade de agir. Explica-se.

Estando em causa direitos que mais não são do que manifestações da própria personalidade, "o reconhecimento da idoneidade para a sua titularidade (capacidade jurídica) desacompanhado do reconhecimento da aptidão para os exercitar (capacidade de agir)"[59] representaria uma limitação injustificável ao desenvolvimento dessa mesma personalidade[60]. Nesses termos, entende a doutrina que o exercício dos direitos de personalidade se dá, *prima facie*, pelo próprio sujeito menor de idade[61/62]. Segundo Rabindranath Capelo de Sousa:

Menoridade, (In)capacidade..., cit., p. 38-40; e Mafalda Miranda Barbosa, *Breves reflexões...*, cit., p. 697-700.

58 Sobre o ponto, Pedro Pais de Vasconcelos entende que "o caráter padronizado da fixação da maioridade no décimo oitavo aniversário é atenuado pela lei em diversos preceitos do Código Civil em que o menor vai adquirindo capacidade por patamares etários". Segundo o autor, é possível descortinar na lei estádios diferentes de maturidade: "aos sete anos, segundo o artigo 488.º, n.º 2 do Código Civil, cessa a presunção de inimputabilidade do menor; os artigos 1981, n.º 1, a) e 1984.º prevêem o consentimento do menor de doze anos para a sua adoção; [...] para celebrar o contrato de trabalho, o menor alcança capacidade, em princípio, aos dezasseis anos, embora tal possa suceder aos catorze em casos especiais; também aos dezasseis anos o menor adquire capacidade de gozo para casar (artigo 1601.º do Código Civil), cessa a sua inimputabilidade penal (artigo 19.º do Código Penal), adquire capacidade de exercício quando tenha casado e ainda, no caso do artigo 127, n.º 1, alínea a), para atos de administração e disposição dos bens que tenha adquirido pelo seu trabalho", *vide* Pedro Pais De Vasconcelos; Pedro Leitão Pais De Vasconcelos, *Teoria Geral...*, cit., p. 117-118.

59 Rosa Martins, *Menoridade, (In)capacidade...*, cit., p. 61.

60 Rosa Martins, *Menoridade, (In)capacidade...*, cit., p. 99 e ss.

61 Para Menezes Cordeiro "uma regra geral de incapacidade é, ainda, inaplicável ao exercício de muitos outros direitos, com relevo para os direitos da personalidade e os direitos fundamentais. O menor tem, seguramente, o direito à intimidade da vida privada, pelo menos a partir da adolescência. Além disso, ninguém pode dispor dos seus direitos à vida ou integridade pessoal, invocando representação legal, salvo nos casos em que isso se imponha no interesse estrito do próprio menor – vg., uma intervenção cirúrgica necessária", *vide* António Menezes Cordeiro, *Tratado de direito civil, Vol. 4: Pessoas*; colab. A. Barreto Menezes Cordeiro, 5ª. ed., Coimbra, Almedina, 2019, cit., p. 483.

62 Isso não quer dizer, contudo, que o próprio conteúdo dos direitos de personalidade não possa sofrer limitações pelo fato de o seu titular ser menor de idade. Como bem acentua Mafalda Barbosa, "a menoridade do sujeito titular dos direitos de personalidade pode conduzir a certas limitações específicas de tais posições jus-subjetivas, desde logo porque, enquanto menor, a pessoa está sujeita ao dever de obediência em relação aos pais.

> O exercício dos direitos de personalidade, dada a sua absolutez e eficácia *erga omnes*, processa-se normalmente através de atos materiais ou atos jurídicos, sem caráter negocial. Aliás, o exercício normal, direto e imediato da generalidade dos direitos de personalidade reveste caráter pessoal, cabendo por isso aos menores não podendo tais direitos ser diretamente exercidos pelo representante legal, sem prejuízo da legitimidade deste em matéria de reação perante a ofensa ou ameaça de ofensa de tais direitos[63].

De outro lado, em contraposição à norma genérica do art. 123.º, do CC, o direito português previu autênticos espaços de autonomia à criança e ao adolescente, de acordo com seu grau de amadurecimento e discernimento[64]. Para tanto, lançou mão de múltiplas técnicas legislativas, dentre as quais destacam-se as exceções à incapacidade, albergadas no art. 127.º, do CC[65], e a instituição das ditas "maioridades especiais"[66].

Percebe-se, pois, a existência de um sistema normativo que identifica nos jovens uma autonomia que lhes é própria, afinada ao seu estádio de desenvolvimento, a eles sendo reconhecido "um inalienável direito de participa-

---

A específica estrutura deste dever, como contraponto do exercício das responsabilidades parentais pode implicar, por exemplo, limitações ao direito à privacidade (embora não à sua anulação), ao direito à liberdade de escolha, à liberdade de movimentos, entre outros", *vide* Mafalda Miranda Barbosa, *Breves reflexões...*, cit., p. 691, nota n.º 7. O assunto será oportunamente abordado no tópico 4.

63 Rabindranath Capelo De Sousa, *Teoria Geral do Direito Civil*, vol. II, nota n.º 12 *Apud* Mafalda Miranda Barbosa, *Breves reflexões...*, cit., p. 692, nota n.º 11.

64 *Vide* nota n.º 58.

65 Segundo Menezes Cordeiro, "o artigo 127.º, apesar de epigrafado 'exceções à incapacidade dos menores', estabelece termos tão amplos que inverte, de certo modo, o dispositivo legal, acabando por admitir uma lata capacidade. Alterando a ordem das alíneas do artigo 127.º/1, verifica-se que o menor pode celebrar: os negócios jurídicos próprios da sua vida corrente, ao alcance da sua capacidade natural e que impliquem despesas ou disposições de bens de pequena importância – 127.º/1,b) ; os negócios jurídicos relativos à profissão, arte ou ofício que tenha sido autorizado a exercer e os praticados no exercício dessa profissão, arte ou oficio – 127.º/1, c); os negócios relativos à administração ou disposição de bens que o menor de dezasseis anos tenha adquirido pelo seu trabalho – 127.º/1, a)", *vide* António Menezes Cordeiro, *Tratado de direito...*, cit., p. 479

66 A expressão é utilizada por Guilherme de Oliveira para se referir às várias normas que reconhecem plena capacidade de decisão aos menores: "refiro-me ao art. 1886.º, que dá poderes de decisão livre, em matéria de escolha de religião, ao jovem com dezesseis anos; ao art. 1901.º, n.º 2, que obriga o juiz a ouvir a opinião do menor que tenha catorze anos [com o advento da Lei n.º 61/2008, este preceito deixou de se referir a um limite de idade], quando tiver de diminuir um desacordo entre os progenitores, em assuntos importantes relativos ao poder paternal; ao art. 1981.º, n.º1, alínea a, que exige o consentimento do adoptando com mais de doze anos; ao art. 1931.º, n.º 2, que manda pedir opinião, ao menor com mais de catorze anos, sobre quem há-de ser o seu tutor; [...] Refiro-me ainda à conhecida norma que dá aos menores capacidade de exercício de direitos para a prática de actos jurídicos de 'pequena importância' (art. 127.º, do Código Civil)". Cf. Guilherme De Oliveira, "O acesso dos menores aos cuidados de saúde" *in Revista de Legislação e Jurisprudência*, ano 132, n.º 3898, 1999, cit., p. 16.

ção"[67] nos assuntos familiares. Nessa ótica, assume especial relevância a solução inovadora do art. 1901.º, n.º 3, do CC – notadamente após a redação conferida pela Lei n.º 61/2008 e a eliminação do limite dos catorze anos como idade mínima –, que determina a audição das crianças e dos adolescentes "como regra na decisão de questões que lhe digam respeito"[68]. Mais uma vez, nos valemos dos ensinamentos de Maria Clara Sottomayor:

> Na relação com os pais, os filhos menores deixam de estar sujeitos ao "poder paternal" enquanto dever de obediência a uma autoridade hierarquicamente superior, para serem tratados pela lei como pessoas por cujo desenvolvimento os pais são responsáveis, constituindo a parentalidade não uma relação de poder, mas uma relação afetiva modelada por deveres recíprocos de respeito, auxílio e assistência (artigo 1874.º do Código Civil), em que as crianças têm voz nos assuntos familiares (artigo 1901.º, n.º 3, do Código Civil) e gozam de uma autonomia condicente com a sua idade e maturidade (artigo 1878.º, n.º 2, 2.ª parte, do Código Civil). Este modelo de família impõe aos pais um dever positivo de respeito pela personalidade dos filhos, pelas especificidades do seu temperamento e maneira de ser, permitindo às crianças desenvolverem espírito crítico e serem elas próprias. A lei reconhece, assim, os dados da psicologia e da antropologia, de acordo com os quais as crianças não são seres passivos e irracionais, mas seres em desenvolvimento, que contribuem de forma ativa para a construção das normas educativas e sociais que orientam a sua vida.[69]

Daqui, chega-se a um eventual ponto de tensão. Em paralelo à exigência de promoção e respeito pelo direito ao livre desenvolvimento da personalidade do sujeito menor de idade, situa-se "o direito e interesse fundamental dos pais (correspondendo também à plena realização da personalidade destes)"[70], de cuidarem e educarem os filhos.

É precisamente da busca pelo ponto de equilíbrio entre as responsabilidades dos pais e a independência progressiva da criança e do adolescente que nos ocuparemos no capítulo em seguida.

---

67 Rui Assis, *A reforma do direito...*, cit., p. 145.

68 Helena Gomes De Melo [ET AL], *Poder paternal e responsabilidades parentais*, 2.ª ed., Lisboa, Quid Juris, 2010, cit., p. 37. Apesar da literalidade do art. 1901.º, n.º 3, do CC referir-se à necessidade de audição do filho apenas "em caso de pais casados e que não cheguem a acordo sobre questões da vida do filho", os autores entendem que, "mesmo em caso de acordo, existe um dever genérico de audição". Consoante evidenciam, essa interpretação deriva do próprio espírito da lei ordinária, bem como do paradigma proposto pelo art. 12.º, n.º 1 da Convenção de Nova York sobre os Direitos da Criança, *vide* p. 40.

69 Maria Clara Sottomayor, *Interesse da criança...*, cit., p. 2-3.

70 Raul Guichard, *Sobre a Incapacidade...*, cit., p. 109.

3. AS RESPONSABILIDADES PARENTAIS COMO INSTRUMENTO AO SERVIÇO DO CUIDADO DA CRIANÇA E DO JOVEM

Da percepção do exercício da parentalidade nos moldes contemporâneos, sobressai a preocupação com a responsabilidade dos pais na construção de um ambiente saudável, democrático e hábil à formação da autonomia do filho em seus vários estágios da vida, o que, nos dias de hoje, certamente engloba o ambiente digital.

Eis que os problemas decorrentes do equacionamento entre poderes-deveres de supervisão e educação dos pais e o direito ao livre desenvolvimento da personalidade dos filhos também se fazem sentir no mundo cibernético, é essencial entender de que modo o direito se propõe a resolvê-los, esclarecendo-se, inicialmente, o olhar jurídico empregado às responsabilidades parentais, ao seu conteúdo e eventuais limites.

3.1. O CONTEÚDO DAS RESPONSABILIDADES PARENTAIS

À metamorfose da imagem social da criança e do adolescente a partir do seu reconhecimento como pessoa que se perspectiva como um centro autónomo de interesses dotado de (alguma e gradual) autonomia no exercício de direitos e liberdades fundamentais, seguiu-se a necessidade de aprimoramento do que as responsabilidades parentais vêm a encapsular[71].

A evolução do conteúdo das responsabilidades parentais é perceptível tão logo se observa a otimização da terminologia cujo instituto ela se reporta, anteriormente referido "poder paternal".

De acordo com a concepção tradicional, fortemente inspirada pela estrutura familiar patriarcal, o poder paternal era encarado como verdadeiro poder-sujeição, por meio do qual a incapacidade de agir dos filhos menores de idades era suprida[72]. O poder paternal era, assim, reduzido ao mecanismo da representação legal[73], "acompanhado de poderes susceptíveis de serem

---

71 "O estatuto de cidadania social atribuído à criança no século XX e assente no seu reconhecimento como pessoa, sujeito de direitos, dotado de uma autonomia progressiva, coloca, agora no século XXI, o desafio da adequação das responsabilidades parentais a este novo estatuto da criança." Cf. Rosa Cândido Martins, *Responsabilidades parentais...*, cit., p. 25.

72 "[...] ao 'dogma' da incapacidade geral de agir do menor veio a corresponder o 'dogma' do poder paternal como poder-substituição e, consequentemente, o 'dogma' da sujeição do filho menor aos pais." Cf. Rosa MartinS, *Menoridade, (In)capacidade...*, cit., p. 165. Em igual sentido: Sónia Moreira, "A autonomia do menor no exercício de seus direitos" *in Scientia Ivridica*, Tomo L, n.º 291, Braga, Universidade do Minho, 2001, cit, p. 165.

73 Essa realidade era facilmente apreciável a começar pelo lugar reservado para a disciplina do "poder paternal" no Código de Seabra: Título IX (Da incapacidade por menoridade e seu suprimento) da Parte I (Da Capacidade Civil).

exercidos de forma autoritária sobre a pessoa do filho"[74], tais como o poder de guarda e o poder de correção[75].

Todavia, a afirmação da criança como sujeito de direitos, aliada ao processo de desfuncionalização da família e à valorização da solidariedade e do mútuo respeito entre os membros da família nuclear[76], provocou uma mudança da sua posição dentro da estrutura familiar, o que, por sua vez, alterou o entendimento acerca da relação pai-filhos menores de idade[77/78].

Já não é concebível, nos dias hodiernos, a visão do poder paternal como relação de poder do pai face aos filhos menores de idade. Reconhece-se, por isso, que o vocábulo "poder paternal" é inadequado para traduzir a realidade jurídico-social da família[79].

Nessa perspectiva, abraçando a terminologia perfilhada a nível internacional[80], o art. 3.º da Lei n.º 61/2008, de 31 de outubro, veio a estabelecer que "a expressão 'poder paternal' deve ser substituída por 'responsabilida-

---

74 Rosa Martins, *Menoridade, (In)capacidade...*, cit., p 160.

75 Rosa Martins, *Menoridade, (In)capacidade...*, cit., p. 160.

76 "A evolução da família, ao longo dos tempos, mostra-nos que esta tem perdido algumas das suas funções tradicionais. Perdeu a função política que tinha no direito romano, quando se estruturava sobre o parentesco agnatício, assente na ideia de subordinação ou sujeição ao *paterfamilias* de todos os seus membros. Perdeu a função económica de unidade de produção, embora continue a ser normalmente uma unidade de consumo. As funções educativa, de assistência e de segurança, que tradicionalmente pertenciam à família, tendem hoje a ser assumidas pela própria sociedade. [...] A desfuncionalização da família reforçou porém a sua intimidade, e permitiu que se revelassem, por assim dizer, as funções essenciais e irredutíveis do grupo familiar: nas relações entre os cônjuges, a sua mútua gratificação afetiva, e, por outro lado, a socialização dos filhos, ou seja, a transmissão da cultura, como conjunto de normas, valores, 'papéis' e modelos de comportamento dos indivíduos." Cf. Francisco Pereira Coelho; Guilherme De Oliveira, *Curso de Direito da Família,* Vol. I, 5.ª ed., Rui Moura Ramos (colaborador), Coimbra, Imprensa da Universidade de Coimbra, 2018, cit., p. 119-120.

77 Rosa Cândido Martins, *Responsabilidades parentais...*, cit., p. 35.

78 Segundo Guilherme de Oliveira, ao se afastar da orientação tradicional que consagrava apenas aos filhos o dever de respeitar os pais, a passagem do texto do art. 1874.º, n.º 1, do CC que diz que "pais e filhos devem-se mutuamente respeito" significa "uma revolução no modo de entender as relações entre pais e filhos". Cf. Guilherme De Oliveira, *Protecção de menores...*, cit., p. 273.

79 "A palavra 'poder' significa posse, domínio e hierarquia e está em contradição com a actual concepção de família participativa e democrática, baseada na igualdade entre os seus membros e em deveres mútuos de colaboração, de auxílio e de respeito. A palavra 'paternal' refere-se à preponderância do pai que caracterizava a família patriarcal, definida pela posição hierarquicamente superior do chefe masculino, em relação à mulher e aos filhos". Cf. Maria Clara Sottomayor, *O poder paternal...*, cit., p. 44.

80 O vocábulo foi adotado pelo Comité de Ministros do Conselho da Europa em 1984 com a aprovação da Recomendação n.º R(84) 4 sobre Responsabilidades Parentais, encontrando guarida também na Convenção sobre os Direitos da Criança/1989 e na Convenção Europeia sobre o Exercício dos Direitos da Criança/1996. No direito interno, já havia sido utilizado na Lei de Protecção das Crianças e Jovens em Perigo (LPCJP), de Setembro de 1999.

des parentais' em todas as disposições da secção II do capítulo II do título III do livro IV do Código Civil"[81/82]. Muito mais do que simples variação semântica, essa mudança terminológica deixa transparecer o abandono da ideia de uma identidade pessoal entre pais e filhos, segundo a qual estes últimos constituem senão um mero prolongamento ou continuidade dos primeiros, para reconhecer que os filhos "têm o direito ao respeito como pessoas diferentes dos seus pais, no seu feitio peculiar"[83]. A exposição de motivos do projeto que esteve na origem do aludido diploma revela que outra não foi a finalidade do legislador português, lendo-se:

> Na mudança da designação está obviamente implícita uma mudança conceptual que se considera relevante. Ao substituir uma designação por outra muda-se o centro de atenção: ele passa a estar não naquele que detém o poder – o adulto neste caso – mas naqueles cujos direitos se querem salvaguardar, ou seja, as crianças. [...] a designação anterior supõe um modelo implícito que aponta para o sentido de posse, manifestamente desadequado num tempo em que se reconhece cada vez mais a criança como sujeito de direitos.[84]

A densificação do conteúdo funcional e relacional das responsabilidades parentais deve partir, desse modo, dos processos transformativos das relações familiares, por meio dos quais pais e filhos menores de idade deixaram de ser colocados em posições antagônicas para encabeçarem uma relação de compreensão recíproca alicerçada na afetividade.[85]

É tendo como referência esse modelo democrático de família que Maria Clara Sottomayor acolhe a expressão "cuidado parental". Conforme expõe, "o

---

81 O esforço destinado a eliminar a expressão "poder paternal" deixou de fora dispositivos situados externamente à referenciada secção, a exemplo dos arts. 124.º e 1921.º, n.º 1, do Código Civil, que continuam a empregar esse termo.

82 A expressão "responsabilidades parentais" não é ausente de críticas na doutrina. Jorge Duarte Pinheiro entende que o termo "parental" remete a um equívoco. Segundo o autor, "parental, no português jurídico, diz respeito a parentes, ou seja, a pessoas unidas por um vínculo decorrente de uma delas descender da outra ou de ambas procederem de um progenitor comum; ora, as responsabilidades parentais são originariamente exercidas apenas por certos parentes, os pais, parentes do menor no primeiro grau da linha recta ascendente". Reconhece, no entanto, que a mudança de nomenclatura teve o substancial efeito de assinalar o fim de uma época em que se privilegiava o exercício dessas responsabilidades pela figura do pai, *vide* Jorge Duarte Pinheiro, "As crianças, as responsabilidades parentais e as fantasias dos adultos" *in Estudos de homenagem ao Prof. Doutor Jorge Miranda*, Vol. VI, Marcelo Rebelo De Sousa [Et. Al.], Coimbra, Coimbra Editora, 2012, cit., p. 535.

83 Maria Clara Sottomayor, *O poder paternal...*, cit., p. 46.

84 HELENA BOLIEIRO; PAULO GUERRA, A criança e a família – uma questão de direito(s): visão prática dos principais institutos do direito da família e das crianças e jovens, 2.ª ed., Coimbra, Coimbra Editora, 2014, cit., p. 185-186.

85 RITA LOBO XAVIER, "Responsabilidades parentais no séc. XXI" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 5, n.º 10, Coimbra Editora, 2008, cit., p. 17-18. De maneira análoga, Cristina Dias, para quem "o conteúdo do poder paternal modificou-se porque também se criou um novo conceito de família, baseada na afectividade e compreensão dos seus membros". Cf. CRISTINA DIAS, *A criança...*, cit., p. 91.

conceito de cuidado é [...] o centro da relação entre pais e filhos".[86] Esse aspecto relacional das responsabilidades parentais é evidenciado, em primeiro plano, na Lei Fundamental, que privilegia o cuidado da pessoa do filho através da sua manutenção e educação[87] (art. 68.º, n.º 1 c/c art. 36.º, n.º 5, CRP).

Da moldura constitucionalmente estabelecida[88], exsurge o desenho legal das responsabilidades parentais como realidade jurídica multifacetada que engloba o suprimento da incapacidade das crianças e dos jovens, mas a ele não se restringe[89]; de logo, porque coexistem com momentos de capacidade exteriorizados através das ditas "maioridades especiais"[90].

Juridicamente, as responsabilidades parentais emergem como efeito automático e indisponível do vínculo de filiação, materializando-se num conjunto de poderes-deveres, que são atribuídos e impostos a ambos os progenitores com vistas à proteção e promoção do desenvolvimento integral do filho menor de idade não emancipado (art. 1878.º, CC)[91/92]. O caráter funcionalizado é, pois, a marca indelével das responsabilidades parentais, que

---

86 MARIA CLARA SOTTOMAYOR, *O poder paternal...*, cit., p. 44.

87 ROSA MARTINS, *Menoridade, (In)capacidade...*, cit., p. 173.

88 Conforme pontua João de Castro Mendes, os princípios estruturantes das responsabilidades parentais restam definidos nos arts. 36.º e 68.º da Constituição, *vide* JOÃO DE CASTRO MENDES, *direito da família*, edição revista por Miguel Teixeira de Sousa, Lisboa, AAFDL, 1997, cit., p. 338.

89 Defendendo que as responsabilidades parentais não se circunscrevem ao suprimento da incapacidade dos filhos menores, entre outros, *vide* JORGE DUARTE PINHEIRO, *O Direito da Família Contemporâneo*, Coimbra, GESTLEGAL, 7ª ed., 2020, cit., p. 260 e JOÃO DE CASTRO MENDES, *direito da família*, cit., p. 338-339. De maneira semelhante, Rosa Cândido Martins se opõe a essa concepção redutora, que padece de um "erro de perspectiva" ou de um "vício de lógica". Cf. ROSA MARTINS, *Menoridade, (In)capacidade...*, cit., p. 157-168.

90 No que diz respeito às "maioridades especiais", remete-se o leitor ao capítulo precedente, designadamente à nota n.º 66.

91 Nesse sentido: Helena Bolieiro; Paulo Guerra, *A criança...*, cit., p. 177; Rosa Martins, *Menoridade, (In)capacidade...*, cit., p. 176; João De Castro Mendes, *direito da família...*, cit., p. 338-339; Sónia Moreira, *A autonomia do menor...*, cit., p. 166.

92 Questão que se impõe é saber se esses poderes-deveres são enumerados exaustivamente pelo Código Civil. Rosa Cândido Martins entende que "os efectivos poderes-deveres exercitados pelos pais variam necessariamente de acordo com as particulares necessidades do filho, de acordo com o seu próprio processo de desenvolvimento e, por último, de acordo com as reais circunstâncias em que ao filho se encontre". Para Martins, não se há falar em enumeração taxativa pela ordem jurídica, mas tão somente no estabelecimento de "linhas de força" das responsabilidades parentais, *vide* Rosa Martins, *Menoridade, (In)capacidade...*, cit., p. 193. Em sentido contrário, Jorge Duarte Pinheiro entende que "o conteúdo das responsabilidades parentais é típico, coincidindo com aquele que a lei lhe assinala". Segundo expõe, "dado o carácter *erga omnes* das responsabilidades parentais, os terceiros devem estar em condições de saber com segurança quais os domínios em que lhes é vedado interferir", ademais "o grau de funcionalidade das responsabilidades parentais aproxima-as de uma competência de Direito Público, figura cujo conteúdo está legalmente balizado", *vide* Jorge Duarte Pinheiro, *O Direito da Família...*, cit., p. 265.

bem por isso se mostram de todo irrenunciáveis (art. 1882.º, CC) e intransmissíveis (*inter vivos* e *mortis causa*).

Nada obstante seja o seu conteúdo legal ordenado expressamente em torno do interesse da criança – daí porque de conteúdo altruístico, a ordem jurídica não desconhece que o exercício dos poderes-deveres que compõem as responsabilidades parentais integra o direito geral de personalidade dos pais[93].

Trata-se, portanto, de situação jurídica complexa, na qual avultam poderes funcionais, direitos e deveres relativamente à pessoa e aos bens do filho e que perdura por todo o período da menoridade, salvo em caso de emancipação (art. 1877.º, CC)[94].

A relevância do interesse dos progenitores, é bem verdade, é apenas secundária[95], não sendo suficiente para enquadrar as responsabilidades parentais na estrita categoria dos direitos subjetivos[96]. O seu exercício não é

---

93 "A afirmação de uma tal funcionalização do exercício do poder paternal ao interesse do filho não quer significar a anulação completa do interesse dos pais, da realização da sua personalidade através da relação de filiação. Com efeito, o poder paternal tende a exprimir o conteúdo das relações entre pais e filhos menores e estas relações encontram-se hoje baseadas na reciprocidade de sentimentos a que corresponde uma reciprocidade de direitos e deveres." Cf. Rosa Martins, *Menoridade, (In)capacidade...*, cit., p. 191, nota n.º 428. Com igual percepção, Raul Guichard, *Sobre a Incapacidade...*, cit., p. 109.

94 "Com efeito, o poder paternal envolve o poder-dever de velar pela segurança e saúde dos filhos e de dirigir a sua educação (art. 1878.º, n.º 1), de representar o filho (arts. 1878.º, n.º 1, e 1881.º, n.º 1) e de administrar os bens do filho (art. 1878.º, n.º 1; crf. arts. 1888.º a 1900.º), o direito à obediência dos filhos (arts. 128.º e 1878.º, n.º 2) e de utilizar os rendimentos dos bens dos filhos para satisfação das despesas com o sustento, segurança, saúde e educação daqueles (art. 1896.º, n.º 1) e ainda o dever de respeito, auxílio e assistência perante o filho (art. 1874.º, n.º 1) e de prover ao sustento do filho (art. 1878.º, n.º 1). A estas faculdades, direitos e deveres correspondem, relativamente ao filho, as respectivas sujeições, deveres e direitos." Cf. João De Castro Mendes, *direito da família*, cit., p. 338-339.

95 "A finalidade primacial do poder paternal a que se encontram sujeitos os filhos menores consiste em promover o desenvolvimento físico, intelectual e moral destes, com vista à sua autonomia [...], sendo, de algum modo, o interesse dos pais um elemento teleologicamente secundário e os seus poderes instrumentais e limitados." Cf. Raul Guichard, *Sobre a Incapacidade...*, cit., p. 110.

96 "Com efeito, a expressão 'poder paternal' vem-nos dando conta de um 'poder funcional' ou de um 'poder-dever', englobável na ideia de 'direito subjectivo em sentido amplo' (que não na concepção de um direito subjectivo em sentido estrito). Na expressão 'poder paternal' há, pois, 'deveres' (equivalentes grosso modo às 'responsabilidades', mas a par de 'poderes', a maioria dos quais constituem direitos em sentido lato quer relativamente aos filhos (prioritariamente em benefício destes mas também no exercício do direito geral de personalidade dos pais – v.g. no art. 1887.º), quer relativamente a terceiros (máxime em matéria de direitoa da educação dos filhos pelos pais face ao Estado nos termos do art. 36.º, n.º 5, Const.)." Cf. Rabindranath Capelo De Sousa, "As alterações legislativas familiares recentes e a sociedade portuguesa" *in Textos de direito da família para Francisco Pereira Coelho*, Guilherme De Oliveira [coord.], Coimbra, Imprensa da Universidade de Coimbra, 2016, cit., p. 538. Para uma discussão aprofundada acerca da natureza jurídica do instituto, veja-se: Jorge Duarte Pinheiro, *O Direito da Família...*, cit., p. 266-270 e Rosa Martins, *Menoridade, (In)capacidade...*, cit., p. 185-192.

livre e discricionário, ditado pela vontade do sujeito que as exerce; ao contrário, faz-se nos limites e em conformidade com o quadro de direitos e deveres estabelecidos no Código Civil[97]. Nas próximas linhas, vamos nos debruçar mais detidamente sobre os termos em que a lei regula a definição da titularidade e do modo de exercício das responsabilidades parentais.

3.2. A TITULARIDADE DAS RESPONSABILIDADES PARENTAIS E O SEU EXERCÍCIO

Consoante já se deixou antever na secção anterior, as responsabilidades parentais aparecem como efeito da filiação juridicamente estabelecida. Isto significa afirmar que a titularidade dessas responsabilidades está em estreita conexão com o estabelecimento das relações de maternidade e de paternidade[98]. Dito de outro modo: por mero efeito da filiação, os pais são considerados, independentemente da sua vontade, titulares das responsabilidades parentais[99].

Enquanto titulares das responsabilidades parentais, aos progenitores vivos cabe, em regra, o seu exercício[100]. Nesse sentido, orientado pelo art. 36, n.º 3 da CRP[101] e delimitado pela retromencionada Lei n.º 61/2008[102], o sistema jurídico vigente adota a regra segundo a qual o exercício das responsa-

---

97 Rossana Martingo Cruz, "A divulgação da imagem do filho menor nas redes sociais e o superior interesse da criança" *in Direito e Informação na Sociedade em rede: Atas do IV Colóquio Luso-Brasileiro Direito e Informação*, 2016, cit., p. 282.

98 Sobre as regras relativas ao estabelecimento da filiação, *vide* arts. 1796.º e ss. do CC.

99 Helena Bolieiro; Paulo Guerra, *A criança...*, cit., p. 188-189.

100 A lei consagra circunstâncias excepcionais de exercício das responsabilidades parentais por outrem que não os pais, malgrado ainda nessas situações não percam os progenitores a sua titularidade. Quanto ao exercício das responsabilidades parentais por terceiro, *vide* arts. 1903.º, 1904.º, n.º 2 e 1904.º-A, n.º 1 do CC, bem como o art. 27.º, n.º 4 do Decreto-Lei n.º 139/2019 e o art. 7.º, n.º 1, da Lei n.º 103/2009 (Lei do Apadrinhamento Civil).

101 Ao estabelecer que "os cônjuges têm iguais direitos e deveres quanto à capacidade civil e política e à manutenção e educação dos filhos", o art. 36, n.º 3 da CRP representa uma reafirmação pelo legislador constitucional do princípio da igualdade. Consoante expressam Jorge Miranda e Rui Medeiros: "O princípio da igualdade impõe em particular, um princípio de direção conjunta da família, apontando, por isso, para a necessidade de um consenso entre os cônjuges na decisão de questões centrais da vida em comum ou da relação com os filhos". Cf. Jorge Miranda; Rui Medeiros, *Constituição Portuguesa anotada...*, cit., p. 825.

102 No ponto, Jorge Duarte Pinheiro aponta a influência que os Princípios de Direito de Família Europeu Relativo às Responsabilidades Parentais tiveram, apesar de não vinculantes, sobre a Lei n.º 61/2008. Apresentados em 2007 pela Comissão de Direitos da Família Europeu (CEFL), os mencionados princípios visavam "exprimir as soluções mais difundidas nos países europeus em matéria de responsabilidades parentais ou outras soluções tidas como preferíveis", *vide* Jorge Duarte Pinheiro, *As crianças...*, cit., p. 537, nota n.º 12. Em particular, merece destaque o Princípio 3:11, ao dispor que: "os pais com responsabilidades parentais devem ter o mesmo direito e dever de exercer tais responsabilidades e sempre que possível devem exercê-las em conjunto" [tradução livre], disponível em: <URL: http://ceflonline.net/principles/>.

bilidades parentais pertence a ambos os pais, que as exercem em comum[103] (arts. 1901.º, 1906.º, n.º 1, 1911.º e 1912.º, CC).

Convém esclarecer que os contornos desse exercício comum são distintos a depender da situação da relação assentada entre os progenitores.

Se os pais vivem numa comunhão plena de vida, quer na constância do casamento, quer na convivência análoga da união de facto, impera o regime de exercício conjunto pleno das responsabilidades parentais (arts. 1901.º, 1902.º e 1911, n.º 1, CC). Nesse caso, ambos os progenitores exercem os poderes-deveres relativos às responsabilidades parentais de comum acordo[104], decidindo conjuntamente sobre todas as questões da vida do filho.

Na eventualidade de os pais coabitantes discordarem quanto às questões de particular importância[105], abre-se a possibilidade de qualquer um deles recorrer ao tribunal que tentará a conciliação (art. 1901, n.º 2, CC). Não sendo esta possível, o tribunal decidirá, devendo, para tanto, proceder à audição do filho, "salvo quando circunstâncias ponderosas o desaconselhem" (art. 1901.º, n.º 3, CC).

Em caso de vivência apartada dos pais, seja porque estão divorciados, separados ou deixaram de viver em união de facto, seja porque nunca viveram juntos, aplica-se um "modelo de exercício comum mitigado"[106], materialmente distinto. Aqui, as responsabilidades parentais em questões de particular importância para a vida do filho são, em princípio, exercidas em comum por ambos os pais, salvo nos casos de urgência manifesta[107]; no entanto, as relativas aos atos da vida corrente do filho[108], são exercidas exclu-

---

[103] Apenas excepcionalmente o exercício das responsabilidades parentais incumbe a apenas um dos pais, o que ocorre nas seguintes situações: quando há impedimento ou morte do outro progenitor (art. 1903.º, 1904.º e 1911.º, CC); quando a filiação se encontrar constituída somente quanto a um dos pais (art. 1910.º, CC); ou quando os pais não tenham vivência comum e, cumulativamente, o exercício por ambos os pais for contrário ao interesse do filho (art. 1906.º, n.º 2, 1911, n.º2, e 1912, n.º 1, CC).

[104] Atento à realidade da vida quotidiana, o legislador dispõe que se um dos pais coabitantes praticar ato que integre o exercício das responsabilidades parentais, "presume-se que age de acordo com o outro, salvo quando a lei expressamente exija o consentimento de ambos os progenitores ou se trate de acto de particular importância" (arts. 1902.º e 1911, n.º 1, CC).

[105] Conceito indeterminado sobre o qual discorreremos adiante.

[106] Expressão utilizada por Jorge Duarte Pinheiro Cf. Jorge Duarte Pinheiro, *As crianças...*, cit., p. 538.

[107] Como preanunciado na nota n.º 103, sempre que esse exercício comum das responsabilidades parentais pelos pais não coabitantes for contrário ao interesse do filho menor de idade, deve o tribunal determinar que essas responsabilidades sejam exercidas por apenas um dos progenitores (art. 1906.º, n.º 2, 1911, n.º 2, e 1912, n.º 1, CC).

[108] "Os atos da vida corrente do menor são aqueles que concernem ao seu dia-a-dia. Que, atendendo à sua índole rotineira, o seu exercício compartido traria dificuldades decorrentes da recapitulação de determinados atos que, pela sua natureza se repetem frequentemente, sendo inexigível uma atuação conjunta a todo o tempo (que, atendendo à não comunhão de habitação por parte dos pais, seria impraticável)." Cf. Rossana Martingo Cruz, *A divulgação da imagem...*, cit., p. 286.

sivamente pelo progenitor que com ele reside habitualmente (arts. 1906.º, 1911.º, n.º 2 e 1912.º, n.º 1, CC).

Numa e noutra hipótese, mostra-se de especial relevância definir os contornos do que sejam "questões de particular importância". Enquanto conceito indeterminado, sua densificação se dá a partir da valoração das circunstâncias do caso concreto, permitindo-se que a norma "se possa adaptar à variabilidade e a imprevisibilidade das situações da vida, em especial, de cada família"[109]. Nessa perspectiva, a exposição de motivos contida nos trabalhos preparatórios da Lei n.º 61/2008 esclarece que a definição do seu âmbito cabe à jurisprudência[110] e à doutrina[111], pertencendo as questões de particular importância "ao núcleo essencial dos direitos que são reconhecidos às crianças"[112].

Decompostas as balizas legais acerca do exercício das responsabilidades parentais na perspectiva da relação entre os progenitores, é quiçá mais importante para os fins perquiridos pelo presente estudo que seja analisado esse exercício na perspectiva da relação entre pais e filhos. Disso nos ocuparemos na próxima secção.

---

[109] Helder Roque, "Os conceitos jurídicos indeterminados em Direito de Família e a sua integração" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 2, n.º 4, Coimbra Editora, 2005, cit., p. 94.

[110] Em julgado de 27 de janeiro de 2020, o Tribunal da Relação do Porto asseverou que o temo "questões de particular importância" representa um "conceito indeterminado, com a capacidade de abranger um conjunto alargado de situações que uma enumeração taxativa comprometeria", devendo ser casuisticamente preenchido. Para tanto, conforme apontou a Corte, é "pertinente que sirva de critério a esse preenchimento o impacto relevante que a concreta situação tenha na vida da criança". Cf. Acórdão do Tribunal da Relação do Porto de 27/01/2020 (Relator: José Eusébio Almeida), processo n.º 803/13.6T2OBR-D.P1. A seu turno, após reconhecer que a delimitação do que são as questões de particular importância varia "conforme os costumes de cada família concreta e conforme os usos da sociedade num determinado momento histórico", o Tribunal da Relação de Lisboa estipulou um rol exemplificativo nos seguintes termos: "V- Devem considerar-se 'questões de particular importância', entre outras: as intervenções cirúrgicas das quais possam resultar riscos acrescidos para a saúde do menor; a prática de actividades desportivas radicais; a saída do menor para o estrangeiro sem ser em viagem de turismo; a matrícula em colégio privado ou a mudança de colégio privado; mudança de residência do menor para local distinto da do progenitor a quem foi confiado." Cf. Acórdão do Tribunal da Relação de Lisboa de 02/05/2017 (Relator: Pedro Brighton), processo n.º 897/12.1T2AMD-F.L1-1. Ambos os acórdãos disponíveis em <URL: http://www.dgsi.pt/>.

[111] A doutrina aponta como exemplos de questões de particular importância: representação do filho menor de idade em juízo, deslocações para o estrangeiro, escolha de estabelecimento de ensino, educação religiosa do filho com idade inferior a dezesseis anos, intervenção cirúrgica com alguma gravidade, participação em programa de televisão etc. A respeito do tema, *vide* Rita Lobo Xavier, *Recentes alterações ao regime jurídico do divórcio e das responsabilidades parentais*, Coimbra, Almedina, 2010, cit., p. 67; Rossana Martingo Cruz, *A divulgação da imagem...*, cit., p. 286; Jorge Duarte Pinheiro, *O Direito da Família...*, cit., p. 288.

[112] Exposição de Motivos do Projeto de Lei n.º 509/X

3.3. O SUPERIOR INTERESSE DA CRIANÇA E DO ADOLESCENTE COMO VETOR DO CUIDADO PARENTAL EM UM CONTEXTO DE PROMOÇÃO CRESCENTE DA AUTONOMIA

Sob a lupa da relação entre pai/mãe e filho, o exercício das responsabilidades parentais entabula algumas características particulares.

Em primeiro lugar, cumpre observar que a atividade dos pais no exercício dessas responsabilidades nem sempre consiste na prática de atos jurídicos, consubstanciando-se, em verdade, a generalidade da atuação parental em atos materiais quotidianos, como dar de comer, dar banho, levar o filho à escola etc.[113]

Em segundo lugar, conforme sublinha Rosa Cândido Martins, o exercício dos poderes-deveres parentais se reveste de momentos de índole distinta, a refletir a autoridade dos pais – compreendida como atividade de direção, supervisão e imposição de regras – na realização da sua função protetiva e educadora[114]:

> No exercício, por exemplo, do poder-dever de velar pela saúde do filho, os pais impõem ao filho menor uma determinada alimentação por eles reputada como adequada à sua idade e necessidades, muitas vezes contra a própria vontade do filho menor (momento de autoridade); impedem o filho de ingerir produtos alimentares que não se encontrem em boas condições (momento protectivo) e, ao observarem determinados horários, regras de comportamento, etc. no que respeita às refeições, estão também a educar o filho (momento educativo). Estes três momentos percorrem, por assim, dizer, todo o exercício do poder paternal, dotando-o de uma densidade e intensidade relacional muito forte[115].

Em terceiro lugar, o exercício das responsabilidades parentais está legalmente conformado à realização do interesse do filho, que aparece como critério orientador dos poderes-deveres a elas relacionados (art. 1878.º, CC)[116]. Não correspondendo o exercício das responsabilidades parentais a esse interesse, poderá ser retirado ou limitado mediante decisão judicial (art. 36, n.º 6, c/c art. 69, n.º 1, CRP e art. 1915.º, 1918.º e 1920.º, n.º 1, CC)[117].

---

113 "O essencial do conteúdo do poder paternal consiste nos cuidados quotidianos a ter com a saúde, a segurança e a educação da criança". Cf. Maria Clara Sottomayor, *O poder paternal*..., cit., p. 45.

114 Esse é o espírito que permeia o Código Civil. De fato, ao lado de determinar que "os filhos devem obediência aos pais" (art. 1878.º, n 2.º, 1ª parte), o *codex* atribui aos progenitores, entre outros, o poder-dever de dirigir a educação dos filhos e de velar por sua saúde e segurança (art. 1878.º, n.º 1).

115 Rosa Martins, *Menoridade, (In)capacidade*..., cit., p. 220.

116 "A prossecução do interesse do filho menor de idade deve sempre ser o último fim do instituto." Cf. Helena Bolieiro; Paulo Guerra, *A criança*..., cit., p.178.

117 "O ponto nevrálgico da intervenção judicial em sede de regulação do exercício das responsabilidades parentais é a figura da criança, entendida como sujeito pleno de direitos, designadamente o direito de manter relações gratificantes e estáveis com ambos os progenitores, obrigando-os a respeitar e fazerem respeitar esse interesse do menor." Cf. Acórdão do Tribunal da Relação do Porto de 10/02/2022 (Relatora: Aristides Rodrigues de Almeida), processo n.º 3323/18.9T8VFR-A.P1, disponível em <URL: http://www.dgsi.pt/>.

Definir os contornos do que se entende por interesse da criança e/ou jovem é, portanto, tarefa primordial. Mais uma vez, deparamo-nos com um conceito indeterminado, cujo preenchimento se dá através de juízos de valor e de experiência. Pese embora "de conteúdo fluido e variável, só susceptível de ser concretizado quando referido ao interesse de cada criança"[118] concretamente distinguida, pode-se entender como interesse do filho menor de idade àquele que concorre para o harmonioso desenvolvimento da sua personalidade, em seu aspecto físico, moral, intelectual, emocional e social[119].

A plena realização da personalidade do filho é, destarte, a pedra angular do exercício das responsabilidades parentais. Precisamente por isso, o interesse da criança não deve "ser encarado como um limite ao poder dos pais de educarem e manterem os filhos, mas antes como uma parte integrante ou imanente dele, determinando o seu conteúdo"[120] e direcionando o seu exercício. Consequentemente, os poderes-deveres parentais não podem assumir a mesma intensidade durante toda a vida do filho, devendo, ao invés, serem permeáveis ao grau de autonomia e às capacidades em desenvolvimento da criança e do adolescente[121]:

> Os pais, ao exercerem os concretos poderes-deveres que lhes competem, ao tomarem decisões relativamente à pessoa do filho, estão vinculados não só ao respeito pela personalidade deste, naquele momento, mas também ao próprio evoluir da personalidade do filho, deixando-lhe na medida do possível, a liberdade para a sua autoconstrução. Os pais devem, pois, respeitar, nomeadamente, os direitos do filho à reserva da intimidade da vida privada, à integridade física e moral, à imagem, à liberdade de expressão, bem como as

---

118 Rosa Martins, *Menoridade, (In)capacidade...*, cit., p. 221.

119 Em julgado recente, o Supremo Tribunal de Justiça se posicionou no seguinte sentido: "O superior interesse da criança traduz-se num conceito jurídico indeterminado que visa assegurar a solução mais adequada para a criança no sentido de promover o seu desenvolvimento harmonioso físico, psíquico, intelectual e moral, especialmente em meio familiar, sendo, por isso, aferível em função das circunstâncias de cada caso. [...] O superior interesse do filho não é alheio a uma adequada inserção dele no meio familiar de cada um dos progenitores mediante aprendizagem dos novos modos de relacionamento e de respeito mútuo pelos direitos e legítimos interesses de cada pessoa que passe a integrar esses agregados familiares." Cf. Acórdão do Supremo Tribunal de Justiça de 27/01/2022 (Relator: Tomé Gomes), processo n.º 19384/16.2T8LSB-A.L1.S1, disponível em <URL: http://www.dgsi.pt/>.

120 Raul Guichard, *Sobre a Incapacidade...*, cit., p. 110.

121 "Com efeito, mesmo durante a menoridade, o crescimento da criança e a sua crescente capacidade para decidir autonomamente sobre os seus próprios interesses justificam – numa ordem constitucional que considera as crianças e os adolescentes como sujeitos de direitos (e sujeitos de direitos fundamentais) e que, em conformidade repudia o modelo autoritário da completa submissão dos filhos menores aos pais – que, a partir de certa idade, e designadamente na adolescência, o menor adquira capacidade para exercer certos direitos ou, pelo menos, um maior espaço de autonomia juridicamente relevante (*v.g.* participação nas decisões que lhe digam respeito através, designadamente, do direito de ser ouvido)." Cf. Jorge Miranda; Rui Medeiros, *Constituição Portuguesa anotada...*, cit., p. 830.

> escolhas existenciais do filho em matéria de profissão, de ideologia política, de religião, etc.[122]

A concepção do que seja interesse do filho menor de idade não é, por conseguinte, "hetero determinável". À medida em que cresce a sua capacidade para decidir e para se posicionar autonomamente, exige-se um maior espaço de participação do filho na determinação do seu interesse[123].

Aos pais, cumpre ter atenção às opiniões, aos gostos e sentimentos do filho, garantindo-lhe a promoção de esferas de autodeterminação de maneira gradual e consentânea com a sua maturidade. Esta é a solução adotada pela nossa ordem jurídica[124], a única devidamente compatível com o reconhecimento da qualidade de sujeitos de direitos à criança e ao adolescente.

4. *SHARENTING*: O USO NOCIVO DAS REDES SOCIAIS E OS IMPACTOS DA SUPEREXPOSIÇÃO DAS CRIANÇAS E DOS ADOLESCENTES

4.1. A DEMOCRATIZAÇÃO DO ACESSO À INFORMAÇÃO NA SOCIEDADE TELEMÁTICA EM QUE VIVEMOS E O SEU IMPACTO NAS FAMÍLIAS

Nas últimas décadas, com o surgimento da comunicação mediada pelos computadores e pelas comunidades virtuais, não é descomedido afirmar que a humanidade passou a vivenciar uma genuína revolução da tecnologia da informação.

Se a explosão no número de computadores, o crescimento exponencial das suas capacidades, a redução dos seus custos e a disseminação de dispositivos tecnológicos móveis como microcomputadores, *notebooks*, *tablets* e *smartphones* já tornava perceptível a digitalização da organização econômica e social do mundo contemporâneo, com o advento da pandemia da COVID-19, a transição da era analógica para a era digital se tornou de todo irrefutável[125].

---

122 Rosa Martins, *Menoridade, (In)capacidade...*, cit., p. 235.

123 "O envolvimento do filho pelos pais no processo de concretização do seu interesse não se traduz numa qualquer renúncia à competência de decidir, pois são os pais quem efetivamente tomam a decisão; reflecte sim a intenção de preparar o filho para a autonomia, possibilitando-lhe a experiência de um 'processo democrático de decisão', num contexto de diálogo, cooperação e interação essenciais à dinâmica das relações familiares e, em especial, da relação entre pais e filhos." Cf. Rosa Cândido Martins, *Responsabilidades parentais*..., cit., p. 38.

124 O art. 1878.º, n.º 2, segunda parte, do CC, firma que os pais, "de acordo com a maturidade dos filhos, devem ter em conta a sua opinião nos assuntos familiares importantes e reconhecer-lhes autonomia na organização da própria vida."

125 Com a pandemia da COVID-19, o papel dos dispositivos conectados à *Internet* passou do luxo para a necessidade. Ao discorrer sobre o que denomina de "virtualidade real na pós-pandemia", o sociólogo espanhol Manuel Castells afirma que "agora entramos em uma sociedade digital em que já vivíamos, mas que ainda não havíamos assumido", *vide*

O novo normal é o digital. Essa é uma realidade que se expande a cada dia e que não passa distante da vida familiar[126]. Com efeito, todas as áreas de relacionamento intersubjetivo e de realização pessoal do ser humano foram rearranjadas a partir das novas ferramentas de comunicação, e, por óbvio, as relações entre os integrantes da família não se furtaram a essa dinâmica[127].

Serviços como *Zoom*, *Skype*, *Facetime* e *Whatsapp* passaram a integrar o dia a dia da família, facilitando o convívio intrafamiliar, ainda quando inexistente a proximidade física entre os seus membros[128]. Para além disso, a utilização das redes sociais[129] pelos sujeitos familiares tornou-se prática comum nos lares, sendo oportunizado um novo espaço para a manifestação democrática no seio doméstico e para o exercício das liberdades individuais, nomeadamente da liberdade de expressão.

A popularização das mídias sociais representa, talvez, o estágio atual desse processo de adesão social ao mundo digital. Hoje, mais do que uma

---

Manuel Castells, "O digital é o novo normal" *in Fronteiras do pensamento*, 2020, disponível em https://www.fronteiras.com/leia/exibir/o-digital-e-o-novo-normal (01/06/2022).

126 Inquérito à utilização de tecnologias da informação e da comunicação pelas famílias realizado pelo Instituto Nacional de Estatística – *Statistics Portugal* (INE) revelou que, no ano de 2021, 82,3% da população residente em Portugal dos 16 aos 74 anos utilizava a *Internet*. Constatou-se, afora isso, que a percentagem de agregados familiares com ligação à *Internet* em casa através de banda larga continua em crescimento. Segundo o INE, em 2021, essa proporção aumentou em 2,4 pontos percentuais em relação ao ano anterior, sendo agora de 84,1%. Cf. Portugal, Instituto Nacional De Estatística, *Inquérito à utilização de tecnologias da informação e da comunicação pelas famílias, 2021*, disponível em https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=473557834&DESTAQUESmodo=2 (01.06.2022).

127 Conrado Paulino da Rosa defende que o avanço da tecnologia operou mudanças tão profundas na sociedade que se pode, inclusive, construir um novo conceito de família: *iFamily.* Para Rosa, a viabilidade de constituição da família virtual se dá diante das novas formas de afetividade que se tornam possíveis diante dos novos meios de comunicação, *vide* Conrado Paulino Da Rosa, *IFamily: um novo conceito de família?*, São Paulo, Saraiva, 2012

128 Como não poderia deixar de ser, o Direito reconhece essa factualidade. A título de exemplo, em Acórdão julgado por unanimidade, o Tribunal da Relação do Porto confirmou os termos estabelecidos em sentença quanto à regulação do exercício das responsabilidades parentais, dos quais se destaca: "o progenitor poderá contactar com a menor, pelo menos, duas vezes por semana, sem prejuízo dos respectivos horários escolares e de descanso, podendo tais contactos ser efectuados por via telefónica, por *Facebook*, *Skype*, *WhatsApp* ou outros meios similares". Cf. Acórdão do Tribunal da Relação do Porto de 12/10/2021 (Relatora: Anabela Dias da Silva), processo n.º 8369/17.1T8VNG.P1, disponível em <URL: http://www.dgsi.pt/>.

129 "As redes sociais são sítios de *internet* que permitem ao usuário criar e exibir um perfil relatando suas experiências pessoais, publicando suas opiniões, postando vídeos e fotografias, enfim, conversar e interagir com familiares, amigos, colegas de trabalho, da comunidade ou mesmo com desconhecidos. Permite-se com isso a criação de um perfil público (ou semipúblico), a partir do qual haverá compartilhamento e publicações de conteúdos variados". Cf. Bruno Torquato Zampier Lacerda, *Bens digitais*, 2ª ed., São Paulo, Foco, 2021, cit., p. 74.

sociedade de conhecimento, somos uma sociedade de imagem[130], que encontra na visualização de perfis uma de suas válvulas de escape[131].

Ao mesmo tempo em que as redes sociais e as demais tecnologias de informação podem ser instrumentos de aproximação entre as pessoas – e efetivamente os são –, justamente por permitirem a criação de um campo inovador no que diz respeito aos relacionamentos humanos, delas decorrem novos desafios para o direito. Nos próximos tópicos, analisaremos alguns dos riscos que afloram desse ambiente cibernético.

4.2. A POTENCIAÇÃO DE RISCOS DE ATENDADOS AOS DIREITOS DE PERSONALIDADE NA ERA DIGITAL

a) Os riscos da digitalização

Marcas do mundo contemporâneo, a quantidade de informações disponíveis na rede mundial de computadores, a velocidade de sua transmissão e a capacidade de seu armazenamento trouxeram uma nova dimensão de vulnerabilidade ao ser humano. Se por um lado, não se olvidam os incontáveis benefícios e comodidades advindos da evolução das tecnologias da informação; de outro, é de se reconhecer que as novas tecnologias suscitam ameaças e agressões a direitos de personalidade impensáveis em uma era "pré-digital"[132].

---

130 "Vivemos hoje num mundo de imagens. As imagens são como nunca antes utilizadas enquanto forma de comunicação, substituindo a linguagem escrita e mesmo oral." Cf. Maria Raquel Guimarães, "A Tutela da Pessoa e da sua Personalidade: algumas questões relativas aos direitos à imagem, à reserva da vida privada e à reserva da pessoa íntima ou direito ao caráter" *in A tutela geral e especial da personalidade humana – 2017*, 1ª. ed., Lisboa: Centro de Estudos Judiciários, 2018, disponível em https://cej.justica.gov.pt/LinkClick.aspx?fileticket=jEOZNTAE5L0%3d&portalid=30 (14.07.2022), cit., p. 28.

131 Segundo a pesquisa *Digital 2022: Global Overview Report*, publicada em parceria com *We Are Social* e *Hootsuite*, o "típico usuário global da *Internet*" passa cerca de 7 horas por dia conectado, das quais as mídias sociais são responsáveis em média por 2 horas e 27 minutos, 35% do total. A pesquisa revela que os usuários de mídias sociais equivalem a 58,4% da população mundial, sendo esperado que a marca dos 60% seja atingida ainda no ano de 2022. Ademais, conforme indica a investigação, na última década, enquanto o número de internautas subiu de 2,18 bilhões para 4,95 bilhões, o número de usuários de mídias sociais viu um crescimento ainda mais acelerado: de 1,48 bilhões em 2012 aumentou para 4,62 bilhões no início de 2022. Cf. Datareportal, *Digital 2022 Global Digital Overview, 2022*, disponível em https://datareportal.com/reports/digital-2022-global-overview-report (01.06.2022).

132 "No contexto da sociedade de informação, que implica um acesso generalizado a uma pluralidade – sempre crescente de meios de comunicação electrónicos –, bem como da oportunidade de utilização da citada tecnologia para estabelecer relações sociais, os perigos resultantes para o indivíduo são únicos na História". Cf. Alexandre Sousa Pinheiro, *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional*, Lisboa, AAFDL, 2015, cit., p. 828. Caminha em igual sentido, Maria Raquel Guimarães, para quem "os novos meios de comunicação vêm potenciar inúmeros ataques

Na realidade pós-moderna, talvez nenhum âmbito tenha sofrido maior impacto do que a privacidade, em suas múltiplas facetas[133]. A *Internet* permitiu uma ressignificação do espaço e do tempo, de modo que as informações compartilhas na Rede têm um alcance extraordinário. Informações pessoais que estavam, substancialmente, sob o exclusivo controle dos interessados são, hoje, acessíveis a uma pluralidade indeterminada de sujeitos[134] e por um prazo indefinido de tempo[135]:

> Os meios informáticos potenciam extremamente os perigos de intromissão na vida privada. O cruzamento de informações permite a reconstituição nos aspectos mais relevantes socialmente da vida de cada um. Perante o desenvolvimento incessante dos processos informáticos da vida corrente, torna-se uma questão vital a defesa da privacidade face à informática. Cada pessoa passa assim a viver uma espécie de liberdade condicional. Está constantemente exposta, ou dependente de quem a possa expor. A todo momento pode ser liquidada por factos tirados do passado, revelados na medida necessária e no momento oportuno.[136]

A instantaneidade conquistada com o surgimento da *Internet* tornou possível o armazenamento e a divulgação de dados em um patamar de crescimento antes inimaginável[137].

à personalidade humana, em diferentes frentes e, agora, com o impacto de estarmos perante violações com repercussões planetárias." Cf. Maria Raquel Guimarães, *A Tutela da Pessoa...*, cit., p. 27.

133 J. Seabra Lopes, "A proteção da privacidade e dos dados pessoais na sociedade de informação*" in Estudos dedicados ao Prof. Doutor Mário Júlio de Almeida Costa*, Germano Marques Da Silva [Et. Al.], Lisboa, Universidade Católica Portuguesa, 2002, cit., p. 785 e ss.; João Paulo Simões De Almeida, "Os riscos da Internet para a privacidade: o caso português" *in Privacidade e comércio electrónico: Colóquio, Lisboa, Comissão Nacional de Protecção de Dados*, 2000, cit., p. 57 e ss.

134 Lívia Teixeira Leal, "O Cuidado na era digital: as novas facetas da afetividade no mundo tecnológico e seus impactos jurídicos" *in Cuidado e Afetividade: projeto Brasil/ Portugal, 2016-2017*, Tânia Da Silva Pereira [Et Al], São Paulo, Atlas, 2017, cit., p.271.

135 Os resultados em "cache" dos mecanismos de busca permitem o acesso a páginas da *Web*, mesmo após o servidor do *site* não estar mais acessível, *vide* Google, *Ver páginas da Web em cache nos resultados da Pesquisa Google*, disponível em https://support.google.com/websearch/answer/1687222?hl=pt (01/06/2022).

136 José De Oliveira Ascensão, "A reserva da intimidade da vida privada e familiar" *in Revista da Faculdade de Direito da universidade de Lisboa*, Vol. XLIII, n.º 1, Coimbra Editora, 2002, cit., p. 16.

137 Sobre a capacidade da tecnologia para coletar e compilar informações, o historiador Yuval Noah Harari entende que, no Século XXI, impera a cultura do armazenamento de dados, ou como prefere chamar, a "religião do Dataísmo" (D*ataism*): "A religião emergente mais interessante é o Dataísmo, que não venera nem os Deuses nem o homem. – venera os dados." [tradução livre], *vide* Yuval Noah Harari, *Homo Deus: a brief history of tomorrow*, 1st edition, Vintage, 2017, cit., p. 427.

Vivemos na era do *Big Data*[138], na qual empresas privadas e entidades públicas recolhem informações pessoais disponibilizadas pelo indivíduo sempre que, de alguma forma, participa-se da vida digital, realizando-se compras com cartões de crédito, candidatando-se a um emprego *online*, fazendo-se uma pesquisa no *Google* etc[139].

O tratamento automatizado de dados não representa, todavia, a única fonte de ameaças à privacidade dentro do contexto digital. Isso porque, a *Internet* trouxe um novo ambiente para a expressão do pensamento, transformando "cada cidadão em um provedor de informação em potencial"[140].

Nesse contexto, a utilização das redes sociais assume especial relevância, seja por impulsionar uma verdadeira democratização na divulgação das informações, seja em razão do próprio conteúdo das informações divulgadas, em sua maioria relacionado ao quotidiano e à vida privada do usuário.

b) Os riscos sobre a privacidade infanto-juvenil em especial

Consoante exposto *supra*, o advento das mídias sociais representou a ultrapassagem da fronteira de privacidade anteriormente estabelecida. Essa afirmação torna-se ainda mais contundente sob a perspectiva da criança e do adolescente, cujo aparecimento nas redes sociais é, não raras vezes, involuntário[141].

Fotos e histórias familiares que outrora eram reservadas para álbuns físicos de fotografia, diários pessoais e trocas de experiências em conversas presenciais passaram a estar disponíveis *online* para um número imensurável de pessoas[142].

O exercício da parentalidade converteu-se em "uma experiência compartilhada digitalmente pelos pais"[143], que documentam, com crescente fre-

---

138 "*Big Data* são as grandes quantidades de informações passíveis de coleta e armazenamento em grande escala. Usando esses dados, empresas e pesquisadores podem implantar algoritmos complexos e tecnologias de inteligência artificial para revelar padrões comportamentais, tendências, identidades e conhecimento prático." [tradução livre] Cf. Anita L. Allen, "Protecting One's Own Privacy in a Big Data Economy" *in Harvard Law Review Forum*, Vol. 130, 2016, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894545 (17.06.2022), cit, p. 71.

139 Anita L. Allen, *Protecting One's...*, cit., p.71.

140 Expressão cunhada por Marques, para quem "é como se a *internet* tivesse colocado todos 'em cima do palco', no 'palanque', com microfones e autofalantes". Cf. Paula Cristina Mariano Marques, "Proteção ao direito de imagem da criança e do adolescente na internet" *in 3º Congresso Internacional de Direito e Contemporaneidade*, 2015, disponível em http://coral.ufsm.br/congressodireito/anais/2015/2-11.pdf (17.06.2022), cit., p. 3.

141 Shannon Sorensen, "Protecting Children's Right to Privacy in the Digital Age: Parents as Trustees of Children's Rights" *in Children's Legal Rights Journal,* Vol. 36, n.º 3, 2020, disponível em https://lawecommons.luc.edu/clrj/vol36/iss3/2/ (20.09.2021), cit., p.156.

142 Shannon Sorensen, *Protecting Children's...*, cit., p. 156-157.

143 Ana Carolina Brochado Teixeira; Renata Vilela Multedo, "(over)Sharenting e o abuso da conduta dos pais no ambiente digital" *in Direitos das Famílias e Sucessões na Era*

quência, a vida das crianças no espaço virtual[144]. A esse fenômeno, dá-se o nome de *sharenting*[145].

Decerto, a exposição de dados pessoais do filho é, por si mesma, apta a bulir com os direitos de personalidade da criança. Imagine-se, por exemplo, a hipótese em que os pais reproduzem, ainda que para um círculo diminuto de pessoas, uma fotografia que a criança não queria que fosse divulgada[146]. Essa contextura se agrava sobremaneira frente ao potencial maximizador da *Internet* e das redes sociais.

Como resultado da hiperexposição dos filhos menores de idade nas aplicações da *Internet* pelos pais, tem-se a criação de um rastro cibernético que tem o potencial de acompanhar os jovens ao longo da sua vida[147] e que se faz, usualmente, independentemente de consentimento[148], interferindo na

Digital, Ana Carla Harmatiuk Matos [Et Al], Belo Horizonte, Instituto Brasileiro de Direito de Família – IBDFAM, 2021, cit., p.316

144 Para BROSCH, a partilha das alegrias e dos desafios da parentalidade pode ser vista, hodiernamente, quase como uma norma social, *vide* Anna Brosch, "When the Child is Born into the Internet: Sharenting as a Growing Trend among Parents on Facebook" *in The New Educational Review*, Vol. 43, n.º 1, 2016, disponível em https://tner.polsl.pl/issues/volume-432016 (20.09.2021), cit., p. 226. Reportagem publicada pelo jornal *The Guardian* é bastante ilustrativa nesse ponto. Entrevistada para a matéria, uma mãe explicou o porquê de ter publicado algumas fotos das filhas nas redes sociais apesar de se preocupar com a privacidade delas: "Suponho que eu só queria provar que sou uma boa mãe. Preocupa-me que, ao não mencionar minhas filhas, as pessoas pensarão que não estou interessada nelas e que não faço coisas com elas. Eu postei uma foto delas e obtive 30 'curtidas'..não pude deixar de me sentir orgulhosa". [tradução livre]. Cf. Nione Meakin, "The pros and cons of 'sharenting'", *in The Guardian*, 2013, disponível em https://www.theguardian.com/lifeandstyle/2013/may/18/pros-cons-of-sharenting (10/06/2022).

145 Decorrente da união das palavras "sharing" (compartilhamento) e "parenting" (enquanto ato de criação dos filhos), *sharenting* é uma expressão da Língua Inglesa que se refere ao hábito de os pais utilizarem excessivamente as mídias sociais para compartilharem informações, fotos e vídeos sobre os seus filhos, *vide* Collins Dictionary, *Sharenting*, disponível em https://www.collinsdictionary.com/submission/11762/Sharenting (01/06/2022); e URBAN DICTIONARY, *Sharenting*, disponível em https://www.urbandictionary.com/define.php?term=Sharenting (01/06/2022)

146 A respeito dos direitos de personalidade do sujeito menor de idade que podem ser afetados pelo *sharenting* e da importância do consentimento no campo da limitação dos direitos pessoais, falaremos adiante (item "c" do tópico 4.2). Veja-se, igualmente, o item "b" do tópico 2.2. do presente estudo.

147 Kate Hamming, "A Dangerous Inheritance: A Child's Digital Identity" *in SEATTLE U. L. REV.*, Vol. 43, n.º 3, 2020, disponível em https://digitalcommons.law.seattleu.edu/sulr/vol43/iss3/7/ (20.09.2021), cit., p. 1037.

148 Uma pesquisa empreendida em 2010 constatou que 81% das crianças de 10 países de alta renda (Austrália, Canadá, França, Alemanha, Itália, Japão, Nova Zelândia, Espanha, Reino Unido e Estados Unidos) tinha algum tipo de perfil ou pegada digital antes mesmo de completar 2 (dois) anos de idade, *vide* Unicef, *THE STATE OF THE WORLD'S CHILDREN 2017: Children in a digital world*, disponível em https://www.unicef.org/media/48581/file/SOWC_2017_ENG.pdf (01.06.2022).

capacidade das crianças e dos adolescentes moldarem a sua própria identidade digital[149]:

> As crianças não apenas têm interesse em proteger informações negativas sobre si mesmas no *feed* de notícias de seus pais, mas também podem não concordar com a decisão dos pais de compartilhar qualquer informação pessoal – negativa ou positiva – sobre eles no mundo online. Não há um *link* de 'opt-out' para crianças e decisões tomadas em frações de segundo por seus pais resultarão em pegadas digitais indeléveis. Enquanto os adultos têm a capacidade de definir seus próprios parâmetros ao compartilhar suas informações pessoais no mundo virtual, as crianças não têm o mesmo controle sobre sua pegada digital, a menos que existam limites para os pais[150]. [tradução livre]

Diante desse cenário, as preocupações com a reserva da intimidade, da vida privada e da imagem da criança, que se centravam na sua exposição por terceiros, foram alargadas para contemplar, em maior medida[151], a privacidade intrafamiliar ou, mais especificamente, a privacidade do filho vis-à-vis seus pais[152].

A formação de um catálogo virtual de dados pessoais da criança pelos pais[153] traz à tona questões tormentosas ligadas ao risco de exposição dos

---

149 Em matéria para a BBC News, Konrad Iturbe, um desenvolvedor de *software* de 19 anos na Espanha, disse ter tido uma "grande revelação aos 14 anos", quando percebeu que os pais postavam fotos dele *online*. Iturbe arfimou que as imagens da sua infância representavam "uma coisa muito íntima" e que, por isso, não se sentia confortável com o seu compartilhamento, acrescentando estar precocupado com "algoritmos de reconhecimento facial" e com a possibilidade de "começar a ser rastreado quando ficar mais velho", *vide* Chelier Cheung, "Publicar fotos dos filhos nas redes sociais é invasão de privacidade?", *in BBC NEWS*, 2019, disponível em https://www.bbc.com/portuguese/geral-47731061 (06/06/2022).

150 Stacey B. Steinberg, "Sharenting: Children's Privacy in the Age of Social Media" *in Emory Law Journal*, Vol. 66, n.º 4, 2017, disponível em https://scholarlycommons.law.emory.edu/elj/vol66/iss4// (20.09.2021), cit., p. 843-844. Sobre a imposição de limites aos pais, debateremos adiante (tópico 4.3.).

151 Não se ignora que a privacidade dos filhos em relação aos progenitores já era objeto de debates jurídicos, mormente em razão do dever de vigilância desses últimos. No entanto, se antes do fenômeno cibernético as discussões se centravam na possibilidade de os pais lerem os diários dos filhos ou abrirem as suas mochilas escolares, na contemporaneidade, essas questões foram redimensionadas.

152 Para usar a expressão de SHMUELI e BLECHER-PRIGAT ("children's privacy vis-à-vis their parents"), *vide* Benjamin Shmueli; Avelet Blecher-Prigat, "Privacy for Children" *in Columbia Human Rights Law Review*, Vol. 42, n.º 3, 2011, disponível em https://heinonline.org/HOL/P?h=hein.journals/colhr42&i=765 (20.09.2021), cit., p. 763.

153 Pesquisa realizada em 2015 com pais poloneses usuários do *Facebook* apurou que, em 90,5% das 168 contas investigadas, constava o primeiro nome da criança e, em 83,9%, a sua data de nascimento. Além disso, em 32,7% dos casos, era possível verificar vídeos ou documentos relativos à criança, como certidão de nascimento ou diploma de jardim de infância, *vide* Anna Brosch, *When the Child...*, cit., p. 229.

jovens à vigilância eletrônica indesejada[154], bem como à captura e à manipulação de imagens por terceiros[155].

Conquanto muitos progenitores sejam iludidos por uma falsa sensação de segurança de que as informações compartilhadas não serão conhecidas senão por audiência por eles previamente selecionada, a realidade é que, ainda quando publicadas em "perfis fechados"[156], as postagens em rede social têm aptidão para atingir um grande público, já que sempre podem ser salvas e repostadas em sítios alternativos[157/158]. Como consequência, são cada vez mais recorrentes relatos de "sequestro digital"[159] e, em casos mais

---

154 De acordo com pesquisadores da Universidade de Nova York (NYU), *data brokers* representam uma ameaça à privacidade das crianças: "os corretores de dados criam perfis sobre as pessoas e os vendem para anunciantes, *spammers*, distribuidores de *malware*, agências de emprego e escritórios de admissão em faculdades. Como o mercado de mercadorias para bebês e crianças está na casa das centenas de bilhões de dólares apenas nos EUA, não é de surpreender que os corretores de dados já estejam procurando compilar dossiês sobre crianças. Usando as informações que os pais postam sobre seus filhos, os corretores de dados podem criar mini-perfis que podem ser continuamente aprimorados ao longo da vida de um indivíduo." [tradução livre]. Cf. Tehila Minkus; Kelvin Liu; Keith W. Ross, "Children Seen But Not Heard: When Parents Compromise Children's Online Privacy" *in WWW'15: 24th International World Wide Web Conference*, 2015, disponível em https://dl.acm.org/doi/pdf/10.1145/2736277.2741124 (13.06.2022), cit., p. 777.

155 Stacey B. Steinberg, *Sharenting: Children's Privacy...*, cit., p. 848-849.

156 Redes sociais como *Facebook* e *Instagram* permitem ao usuário ajustar as configurações de privacidade da sua página, tornando o seu perfil "fechado". Nesta hipótese, para visualizar as publicações, cada novo seguidor deve ser aprovado individualmente pelo titular da conta.

157 Stacey B. Steinberg, *Sharenting: Children's Privacy...*, cit., p. 850.

158 Marques destaca a aleatoriedade com que as informações ganham publicidade quando compartilhadas na Rede. Consoante expõe, a imprevisibilidade da *Internet* é um fator preocupante a ser considerado: "o usuário comum utiliza a *internet* para divulgar suas ideias pessoais e, muitas vezes, informações particulares, contando com um número relativamente baixo de acessos, que se mantém constante e, em geral, com pouca notoriedade. Porém, uma informação qualquer pode ganhar, inesperadamente, grande repercussão. São os chamados 'memes' ou 'virais'." Cf. Paula Cristina Mariano Marques, *Proteção ao direito...*, p. 5.

159 O sequestro digital (*digital kidnapping* ou *virtual kidnapping*) ocorre quando terceiros usurpam fotos de crianças publicadas nas mídias sociais e as repostam em suas próprias contas, fazendo-se passar pelo jovem ou por seus pais, em verdadeira ficção virtual. Foi o que aconteceu com uma mãe em Atalanta, Estados Unidos. Após publicar uma foto de seu filho de 18 meses de idade no *Facebook*, Lindsey Paris percebeu que havia recebido uma "curtida" de um usuário desconhecido. Ao averiguar, descobriu que esse usuário havia feito da imagem da criança sua foto de página inicial e estava a apresentando como seu próprio filho: "Ela estava fingindo que ele era seu filho e comentando quando ele iria começar a dentição. Seus amigos estavam dizendo que amavam o cabelo dele. Ela o estava tratando como seu e isso era a coisa mais petrificante. Não sabia que as pessoas faziam isso." [tradução livre], *vide* Jennifer O'neill, "The Disturbing Facebook Trend of Stolen Kids Photos", *in Yahoo Parenting*, 2015, disponível em https://www.yahoo.com/news/mom-my-son-was-digitally-kidnapped-what-112545291567.html (10/06/2022)

graves, de apropriação de imagens publicadas em redes sociais por *websites* associados à pedofilia[160].

O *sharenting* também pode expor as crianças e os adolescentes a constrangimentos, nomeadamente *cyberbullying*[161], em razão da divulgação de histórias ou de fotografias que podem ser consideradas embaraçosas[162] e que, diante da possibilidade de redescoberta infinita propiciada pela *web*, podem ser reveladas para além da sua infância e adolescência[163].

---

[160] Segundo investigações da *eSafety Commissioner* (Austrália) relatadas no ano de 2015 pelo *The Sydney Morning Gerald*, fotos de crianças originalmente publicadas em mídias sociais e *blogs* familiares representam até metade do material encontrado em alguns *sites* de compartilhamento de imagens de pedofilia, *vide* Lucy Battersby, "Millions of social media photos found on child exploitation sharing sites" *in The Sydney Morning Gerald*, 2015, disponível em https://www.smh.com.au/national/millions-of-social-media-photos-found-on-child-exploitation-sharing-sites-20150929-gjxe55.html (11.06.2022).

[161] Godinho e Drumond explicam que, ao configurar "a virtualização do *bullying*", o *cyberbullying* se revela como "um dos mecanismos mais cruéis de violação a direitos personalíssimos", "especialmente quando a ofensa é propagada por meio das redes virtuais". Cf. Marteleto Adriano Godinho; Marcela Maia De Andrade Drumond, "Autoridade parental: a autonomia dos filhos menores e a responsabilidade dos pais pela prática de cyberbullying" *in Autoridade Parental: dilemas e desafios contemporâneos*; coordenação de Ana Carolina Brochado, Luciana Dadalto, São Paulo, Editora Foco, 2019, cit., p. 176-177. Brosch cita o caso de um grupo criado no *Facebook,* no qual mães repostavam fotos de crianças com deficiências para serem zombadas, *vide* Anna Brosch, *When the Child...*, cit., p. 227.

[162] Segundo relatório divulgado pela *Family Online Safety Institute* (FOSI) em novembro de 2015, fruto de pesquisa conduzida pela *Hart Research Associates* a partir de dados colhidos junto a 589 pais de crianças de 6 a 17 anos, "entre os pais que têm uma conta de rede social, um a cada cinco (19%) reconhece ter postado algo *online* sobre seu filho que ele pode achar embaraçoso no futuro, 13% dizem que o filho ficou envergonhado por algo que os pais postaram sobre ele *online*, e 10% dizem que o filho pediu para que fosse retirado algo que os pais postaram sobre ele." [tradução livre], *vide* Family Online Safety Institute, *Parents, Privacy and Technology Use*, 17/11/2015, disponível em https://fosi-assets.s3.amazonaws.com/media/documents/Full_Report--Web.pdf (13.06.2022), p. 22. De acordo com outra pesquisa, concluída em 2014 por investigadores da Universidade de Michigan entre 569 pais de crianças de 0 a 4 anos, 80% das mães e 70% dos pais relataram a participação em mídias sociais, dos quais a maioria (74%) afirmou conhecer outro pai que compartilhou informações excessivas sobre o filho na *Internet*, incluindo pais que publicaram informações constrangedores sobre a criança (56%), dados capazes de identificar a localização da criança em um determinado momento (51%) ou fotos da criança que podem ser consideradas inapropriadas (27%), *vide* C.S. Mott Children's Hospital, University Of Michigan System, *Parents on Social Media: Likes and Dislikes of Sharenting*, Vol. 23, n.º 2, 16/03/2015, disponível em https://mottpoll.org/sites/default/files/documents/031615_sharenting_0.pdf (13.06.2022).

[163] A preocupação quanto a capacidade da *Internet* de eternizar informações relativas à criança foi abordada pelo Comitê dos Direitos da Criança da ONU. No Comentário Geral n.º 25 sobre os direitos da criança em ambiente digital, lê-se: "Práticas digitais como o processamento automatizado de dados, criação de perfis, seleção de comportamentos, verificação obrigatória da idade, filtragem de informação e vigilância em massa estão a tornar-se habituais. Estas práticas podem levar à ingerência arbitrária ou ilegal no direito das crianças à privacidade; podem ter consequências adversas sobre as crianças, que podem

Como se vê, as pegadas digitais geradas pelo *sharenting* repercutem nas esferas mais íntimas da pessoa da criança e do adolescente. Sendo inegável a vulnerabilidade da população infantojuvenil no ambiente virtual, é fundamental compatibilizar o exercício da parentalidade e a liberdade de expressão dos pais com os direitos de personalidade dos seus filhos menores de idade.

c) Os instrumentos de tutela dos direitos da personalidade

Os direitos da personalidade "são os direitos essenciais ao desenvolvimento da pessoa, em que se convertem as projeções físicas, psíquicas e intelectuais do seu titular"[164]. Representam emanações da própria dignidade reconhecida ao ser humano[165], tutelando os valores mais significativos do indivíduo[166], seja perante a coletividade, seja perante o Estado[167].

É através dos direitos da personalidade que se opera a proteção jurídica avançada da pessoa[168]. Rigorosamente por isso, não se disputa a sua titula-

continuar a afetá-las em fases posteriores das suas vidas." Cf. Organização Das Nações Unidas, Comité Dos Direitos Da Criança (CRC), *Comentário Geral n.º 25 (2021) sobre os direitos das crianças em relação ao ambiente digital*, 2021, disponível em https://gddc.ministeriopublico.pt/sites/default/files/documentos/pdf/crc-cg25-pt.pdf (13.06.2022).

[164] Cristiano Chaves De Farias; Nelson Rosenvald, *Curso de direito civil: parte geral e LINDB*, 19.ª ed., revista, ampliada e atualizada, Salvador, Ed. JusPodivm, 2021, cit., p. 217.

[165] Luís Roberto Barroso, "Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa" *in Revista De Direito Administrativo*, Vol. 235, 2004, disponível em https://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/45123 (22.06.2022), cit., p.12.

[166] "[...] incidem sobre a própria pessoa ou sobre alguns fundamentais modos de ser, físicos ou morais, dessa personalidade, e que inerem, portanto, à pessoa humana – são direitos das pessoas que tutelam bens ou interesses da sua própria personalidade. Os direitos de personalidade exprimem, na conhecida fórmula de Adriano de Cupis, 'o *minimum* necessário e imprescindível do conteúdo da personalidade'. Tais direitos são, portanto, essenciais, uma vez que a personalidade humana quedaria descaracterizada se a proteção que eles concedem não fosse reconhecida pela ordem jurídica." Cf. Paulo Mota Pinto, *Direitos de personalidade e direitos fundamentais: estudos*, Coimbra, GESTLEGAL, 1ª ed., 2018, cit., p. 478. Similarmente, *vide* Alexandre Sousa Pinheiro, *Privacy e proteção...*, cit., p. 768.

[167] "Os direitos da personalidade são absolutos porque possuem eficácia contra todos (ou seja, são oponíveis *erga omnes*), impondo-se à coletividade, e aos particulares individualmente considerados, o dever de respeitá-los." Cf. Cristiano Chaves De Farias; Nelson Rosenvald, *Curso de direito civil...*, cit., p. 223. Em igual sentido, *vide* Carlos Alberto Da Mota Pinto; António Pinto Monteiro; Paulo Mota Pinto, *Teoria geral...*, cit., p. 209.

[168] Para Orlando de Carvalho, os direitos de personalidade são "direitos sobre a própria Pessoa, a que corresponde não apenas uma obrigação negativa, como nos direitos das coisas, mas uma obrigação de respeito, de conteúdo tanto negativo como positivo". E continua: "sem a pessoa e a tutela da pessoa não só o Direito Civil é acéfalo como qualquer Direito ou Ramo de Direito é uma violência monstruosa". Cf. Orlando De Carvalho, *Teoria Geral...*, cit., p. 264-267.

ridade por parte das crianças e dos adolescentes[169], distinguidos enquanto sujeitos de direito[170].

Nessa perspectiva, os artigos n.º 8.º e 16.º da Convenção sobre os Direitos da Criança de 1989 preveem, respectivamente, o direito da criança a preservar a sua identidade, bem como a sua proteção frente a intromissões arbitrárias na sua vida privada e a ofensas à sua honra e reputação.

Na pós-modernidade, a identidade da pessoa "se prospecta no mundo virtual"[171], o que exige seja viabilizada a proteção da sua personalidade na seara digital, ainda que a ela se reconheçam contornos diferenciados. Indubitável, pois, que os jovens gozam do direito à privacidade, aqui compreendido em sentido amplo[172], também na *web*.

As idiossincrasias da *Internet* apontam não para a superação das normas relacionadas aos direitos à imagem (art. n.º 79.º, n.º 1, CC), à reserva sobre a intimidade da vida privada (art. n.º 80.º, n.º 1, CC) e à proteção de dados[173], senão para a necessidade de se garantir a sua aplicação eficaz diante da vultosa capacidade de difusão desse veículo de comunicação[174].

A regra básica consagrada pelo Código Civil é a de que a imagem da pessoa não pode ser exposta, reproduzida ou lançada no comércio sem o seu

---

169 Maria Raquel Guimarães enfatiza que a tutela conferida à personalidade humana deve abranger a própria evolução desta personalidade, *i.l.*: "A personalidade humana deverá ser protegida pelo direito civil em todas as suas manifestações previsíveis e imprevisíveis, adaptando-se a tutela conferida pelo direito civil à evolução desta personalidade bem como à evolução dos ataques de que poderá ser alvo". Cf. Maria Raquel Guimarães, *A Tutela da Pessoa...*, cit., p. 25.

170 Sobre o reconhecimento da criança e do adolescente como sujeito de direitos, remete-se o leitor às considerações tecidas no tópico 2 do presente estudo.

171 Como bem esclarece Leal, se antes da *Internet* a pessoa era identificada como produto da junção de um elemento intelectivo (alma) com um elemento físico (corpo), hoje a identidade pode ser reimaginada dentro do cenário digital, através de elementos que a individualizam, "como uma fotografia, um *nickname*". Cf. Lívia Teixeira Leal, *O Cuidado na era digital...*, cit., p. 268.

172 Não nos cabe examinar as múltiplas acepções trabalhadas pela doutrina acerca da privacidade. Para o fito do presente trabalho, é suficiente reconhecer o direito à privacidade como gênero ou tipo, do qual variados direitos podem ser decompostos de maneira parcelar, o que sucede, por exemplo, com o direito à imagem, "no que esta tenha a ver com as esferas privada, secreta e íntima". António Menezes Cordeiro, *Tratado de direito...*, cit, p. 271.

173 Trataremos detidamente do direito à proteção de dados na perspectiva dos jovens no primeiro tópico do capítulo subsequente (tópico 5.1.).

174 "O direito à protecção de dados não foi criado num universo cibernético que comportasse a vivência em rede, a socialização electrónica – com maior exposição do sujeito à comunidade – e a proliferação informativa em redes abertas. A 'protecção' pretendida na origem não se transforma num objetivo caduco ou desactualizado, mas antes num entre vários desafios levantados ao Direito para regular os direitos dos titulares de informação pessoal na nova existência cibernética." Cf. Alexandre Sousa Pinheiro, *Privacy e proteção...*, cit., p. 777.

consentimento[175]. Ao permitir a identificação da pessoa retratada, o destino dado à sua imagem "é, de certo modo, um tratamento dado à própria pessoa"[176], pelo que a normativa civilística garante o direito do titular "a controlar a captação e a divulgação do seu 'retrato'"[177]. Não por outro motivo, entende Maria Raquel Guimarães que a forma de agressão mais grave a esse direito é constituída pela divulgação não consentida da imagem, "divulgação essa que pode atingir uma dimensão extraordinária – e prolongada no tempo – quando realizada através da *internet*"[178].

Da mesma forma, nos moldes do art. 80.º, n.º 1, do CC, o direito à reserva sobre a intimidade da vida privada tem por objeto o controle dessa informação[179], definindo-se o seu conteúdo pela confluência da autodeterminação sobre a informação com a esfera privada[180].

O ordenamento jurídico pátrio protege, portanto, o interesse do titular em controlar a tomada de conhecimento e a divulgação de informações e imagens sobre a sua vida privada[181/182], incluindo a circulação desses dados na Rede[183]:

---

175 Cf. António Menezes Cordeiro, *Tratado de direito...*, cit., p. 261. Para quem, "a imagem materializada de uma pessoa é um bem de personalidade fortemente objetivado", *vide* p. 258.

176 António Menezes Cordeiro, *Tratado de direito...*, cit., p. 258.

177 Maria Raquel Guimarães, *A Tutela da Pessoa...*, cit., p. 28. Para Guimarães "a simples captação da imagem não autorizada constitui já uma violação do direito" à imagem. Diferentemente, Paulo Mota Pinto entende que o artigo 79.º do Código Civil parece ter "aderido à tese, defendida em Itália, de que não é em princípio vedado colher o retrato de outra pessoa, apenas O sendo a sua exposição, reprodução ou comercialização". Cf. Paulo Mota Pinto, *Direitos de personalidade...*, cit., p. 551.

178 Maria Raquel Guimarães, *A Tutela da Pessoa...*, cit., p. 29.

179 Para Paulo Mota Pinto, o direito à reserva sobre a intimidade da vida privada "tem, antes, por objecto o controlo de informação sobre a vida privada. O interesse que visa proteger é o interesse em controlar a tomada de conhecimento, a divulgação ou simplesmente a circulação de informação sobre a vida privada – isto é, genericamente, sobre os factos, comunicações ou posições relativos ou próximos do indivíduo ou confidenciais ou reservados –, bem como o interesse na subtração à atenção dos outros (anonimato lato sensu), ou interesse na solidão (na exclusão do acesso físico dos outros à pessoa)." Paulo Mota Pinto, "A limitação voluntária do direito à reserva sobre a intimidade da vida privada" *in Estudos em Homenagem a Cunha Rodrigues*, Vol. 2: Estudos variados, direito comunitário, Jorge Figueiredo Dias [ET AL], Coimbra, Coimbra Editora, 2001, cit., p. 528.

180 Paulo Mota Pinto, *A limitação voluntária...*, cit., p. 529.

181 Alexandre Sousa Pinheiro, *Privacy e proteção...*, cit., p. 528-529.

182 "A vida privada compreende as mais diversas realidades: a origem e a identidade das pessoas; a situação de sua saúde; a sua situação patrimonial; a sua imagem; os seus escritos pessoais; as suas amizades e relacionamentos sentimentais; as suas preferências estéticas; as suas opções políticas e religiosas. A rigor, a vida privada abrangerá tudo o que não seja público e profissional ou social." Cf. António Menezes Cordeiro, *Tratado de direito...*, cit., p. 270.

183 A preocupação com a salvaguarda dos direitos de personalidade da criança na Rede levou à adoção pelo Comitê de Ministros do Conselho da Europa da Recomendação CM/Rec(2018)7, segundo a qual "as crianças têm direito à vida privada e familiar no ambiente digital, o que inclui a proteção de seus dados pessoais" [tradução livre]. Cf. Conselho Da Europa, *Guidelines to respect, protect and fulfil the rights of the child in the digital environ-*

> Parece-nos que a utilização do retrato (*rectius*, a violação do direito à imagem), quando se reproduzam cenas da vida privada das pessoas, constitui um meio gravoso de desrespeito pela privacidade, sendo nestes casos violados simultaneamente o direito à imagem e o direito à reserva.[184]

Sem embargo do que se precisou até aqui, convém anotar que quando aplicado aos sujeitos menores de idade, o direito à privacidade apresenta algumas particularidades em razão das condições peculiares de desenvolvimento físico e psíquico dessas pessoas vulneráveis[185]. Aos pais, cumprem os deveres de educação, vigilância e cuidado, pelo que as crianças e os adolescentes não dispõem de plena autonomia na condução da sua vida[186].

Eventual limitação[187] à privacidade infantojuvenil no exercício da autoridade parental somente se justifica, entretanto, em prol dos interesses dos filhos e sempre com vistas à proteção da sua dignidade[188]. É dizer: das responsabilidades parentais não é possível extrair um direito *tout court* dos pais que lhes permita dispor das informações da vida privada de seus filhos por meros voluntarismos.

---

ment: Recommendation CM/Rec(2018)7 of the Committee of Ministers, 2018, disponível em https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cm-rec20187-of-the-committee-of-ministers.html (15.06.2022).

184 Paulo Mota Pinto, *Direitos de personalidade...*, cit., p. 552.

185 Benjamin Shmueli; Avelet Blecher-Prigat, *Privacy for Children...*, cit., p. 768.

186 Decerto, a menoridade não afeta a titularidade de direitos de personalidade por parte das crianças e dos adolescentes. Contudo, considerando a sua qualidade de pessoa em desenvolvimento, o exercício desses direitos pode ser afetado, devendo-se considerar o grau de maturidade do jovem e o fato de os progenitores exercerem as responsabilidades parentais, compreendidas enquanto feixe de poderes-deveres funcionalizados em prol do interesse da criança. Quanto à titularidade e o exercício dos direitos de personalidade em se tratando de sujeito menor de idade, *vide* item "b" do tópico 2.2.

187 Perceba-se que a "limitação" que aqui nos referimos diz respeito às intromissões por parte dos progenitores na privacidade dos filhos, sempre que estas se mostrem em consonância com o dever de cuidado inerente às responsabilidades parentais.

188 Como ressalta Paulo Mota Pinto, "[...] parece-nos que os representantes poderão interferir na intimidade privada dos incapazes na medida em que isso seja relevante para o correto desempenho dos seus ofícios ou poderes-funcionais – por exemplo, se estiver em causa a educação ou formação moral dos incapazes –, mas sempre tendo em conta a eventual maturidade do incapaz (sobretudo do menor, cujo processo de desenvolvimento implicará um gradual amadurecimento). Para lá desses limites, uma intromissão sistemática e arbitrária na intimidade do incapaz, v. gr., violando o segredo telefónico ou epistolar, pode bem lesar a sua esfera de reserva." Cf. Paulo Mota Pinto, *Direitos de personalidade...*, cit., p. 559-560. Acerca dessa questão, *vide* ponderações realizadas no tópico 3, máxime no ponto 3.3.

4.3. LIBERDADE DE EXPRESSÃO DOS PAIS *VERSUS* DIREITOS DE PERSONALIDADE DA CRIANÇA/JOVEM

Utilizar as redes sociais para compartilhar aspectos da rotina e das experiências da parentalidade constitui uma das vertentes do direito dos pais de se expressarem livremente na contemporaneidade[189].

No entanto, como já se pôde analisar, no exercício da sua liberdade de expressão, os pais estão criando uma identidade digital para os seus filhos no mundo virtual, situação que se agrava quando vem desacompanhada de qualquer consentimento[190]. Numa frase, os pais exercem um direito que é seu (liberdade de expressão), mas que acaba por repercutir na esfera de personalidade dos filhos.

A tensão existente entre a liberdade de expressão dos pais e os direitos de personalidade das crianças e dos adolescentes não significa que deva existir a proibição integral de compartilhamento, pelos primeiros, de informações referentes aos seus filhos. É imprescindível, contudo, o estabelecimento de parâmetros capazes de preservar os valores em conflito.

Conforme evidenciado no tópico anterior, no caso da reprodução de imagens e da divulgação de informações da vida privada do indivíduo, a nossa ordem jurídica exige o consentimento da pessoa a que se refiram. Estando em causa aspectos exteriores ou projeções da personalidade, ainda quando se trate de sujeito menor de idade, sempre que o jovem disponha de maturidade suficiente para avaliar, será ele próprio que deverá prestar a sua anuência[191].

---

[189] Fernando Büscher Von Teschenhausen Eberlin, "Sharenting, liberdade de expressão e privacidade de crianças no ambiente digital: o papel dos provedores de aplicação no cenário jurídico brasileiro" *in Revista Brasileira de Políticas Públicas*, Brasília, Vol. 7, n.º 3, 2017, disponível em https://doi.org/10.5102/rbpp.v7i3.4821 (20.09.2021), cit., p. 257.

[190] São nítidos os interesses em conflito. Se de um lado os acadêmicos da Universidade de Granada observaram que para 63,3% dos 367 adultos entrevistados, "o ato de compartilhar *online* as imagens do filho menor de idade não implica invasão ao direito à privacidade da criança" [tradução livre]; de outro, uma pesquisa conduzida, em 2020, com 68 crianças suecas concluiu que "crianças e jovens, independentemente da idade, queriam que os pais lhes perguntassem antes de tirar fotos ou compartilhar imagens deles" [tradução livre]. Cf. Francisco Javier Hinojo-Lucena [Et Al], "Sharenting: Internet addiction, self-control and online photos of underage children" *in Comunicar – Media Education Research Journal*, n.º 64, Vol. XXVIII, 2020, disponível em https://doi.org/10.3916/C64-2020-09 (20.09.2021); e Anna Sarkadi [Et Al], "Children want parents to ask for permission before sharenting" *in Journal of Paediatrics and Child Health*, 56, 2020, disponível em https://doi.org/10.1111/jpc.14945 (20.09.2021). Situação real reflete bem essa contextura. Após a atriz Gwyneth Paltrow publicar uma foto com a filha de 14 anos em seu *Instagram*, sua filha comentou "Mamãe, discutimos isso. Você não pode postar nada sem o meu consentimento", para o que Paltrow respondeu "Nem dá para ver seu rosto!", *vide* CHELIER CHEUNG, "Publicar fotos dos filhos nas redes sociais é invasão de privacidade?", *in BBC NEWS*, 2019, disponível em https://www.bbc.com/portuguese/geral-47731061 (06/06/2022).

[191] "A solução não deve, a nosso ver, depender diretamente da qualificação do consentimento como negócio jurídico, mas sim guiar-se sobretudo pela natureza dos interesses em questão, que se prendem com bens da personalidade. Assim, se, em geral, quanto ao

Não se pode negligenciar, todavia, a posição dos progenitores como primeiros guardiões da identidade digital dos filhos no exercício legítimo das responsabilidades parentais[192]. Em verdade, o compartilhamento das experiências pessoais na *Internet* traz benefícios para a unidade familiar que precisam ser levados em consideração.

Ao compartilhar nas mídias sociais, os pais oferecem aos filhos redes positivas de apoio, convidando familiares e amigos para suas vidas diárias[193]. Além disso, proporciona-se um espaço onde as famílias auxiliam umas às outras no desempenho da parentalidade[194], evitando-se o isolamento social causado por situações desafiadoras próprias da maternidade ou paternidade[195].

A prática moderada do *sharenting*, limitada a postagens e fotos no contexto familiar[196] pode se mostrar condizente com a visão hodierna da parentalidade enquanto cuidado parental, ao mesmo tempo em que cultural e socialmente aceitável[197].

---

exercício e defesa dos seus direitos, os incapazes terão de ser representados de acordo com as regras de suprimento de incapacidades de exercício, o mesmo pode não valer para o acordo para a limitação voluntária de direitos de personalidade de menores. [...] impõe-se que, caso o incapaz (designadamente, o menor) disponha já de maturidade suficiente, não possam ser os representantes, mas antes o próprio menor a ter que dar, ele próprio o seu acordo. Trata-se da limitação de direitos que tutelam bens pessoais, pelo que se exigirá, nomeadamente, o consentimento do próprio menor para a sua limitação, se ele já tiver maturidade suficiente para a avaliar". Cf. Paulo Mota Pinto, *A limitação voluntária...*, cit., p. 542-543.

192 Fernando Büscher Von Teschenhausen Eberlin, *Sharenting, liberdade de expressão...*, cit., p. 259; Ana Carolina Brochado Teixeira; Renata Vilela Multedo, *(over) Sharenting e o abuso...*, cit., p. 326.

193 Stacey B. Steinberg, *Sharenting: Children's Privacy...*, cit., p. 855.

194 Anna Brosch, *When the Child...*, cit., p. 227. Em pesquisa coordenada pelo *Pew Research Center* em 2014, notou-se que 59% dos pais que utilizam as mídias sociais indicaram que se depararam com informações úteis relativas ao exercício da parentalidade nos 30 dias antecedentes à entrevista. Além disso, 42% desses pais afirmaram terem recebido, nos 30 dias antecedentes à entrevista, apoio social ou emocional em suas redes sociais quanto a um problema relacionado à parentalidade. Cf. Maeve Duggan [Et Al], *Parents and Social Media,* Pew Research Center, 2015, disponível em http://www.pewinternet.org/2015/07/16/parents-and-social-media/ (20.09.2021).

195 "Ao compartilhar, as famílias com crianças medicamente frágeis podem se conectar umas com as outras. Essas famílias quebram estereótipos, ajudam a arrecadar dinheiro para causas e pesquisas importantes e muitas vezes recebem apoio pessoal positivo da comunidade." [tradução livre] Cf. Stacey B. Steinberg, *Sharenting: Children's Privacy...*, cit., p. 852.

196 Definir o que se entende por "moderado" na conjuntura do *sharenting* não é tarefa fácil. Parece claro, todavia, que a sua qualificação como tal depende da análise de critérios quantitativos e qualitativos. Assim, não somente o número e a frequência das publicações devem ser sopesados, mas o conteúdo em si das fotos, vídeos e informações compartilhadas. Defendendo igual posicionamento, *vide* Ana Carolina Brochado Teixeira; Renata Vilela Multedo, *(over)Sharenting e o abuso...*, cit., p. 336.

197 O Tribunal de Justiça do Estado de São Paulo/BR entendeu que não houve violação ao direito de privacidade da criança em caso no qual a mãe efetuou publicação no *Facebook*, compartilhando os seus sentimentos ao descobrir o autismo do filho. Nada obs-

Por esse motivo, Ana Carolina Brochado Teixeira e Renata Vilela Multedo preferem utilizar a expressão *oversharenting*, sinalizando que a conduta dos pais no ambiente digital se transmuda em abusiva quando há a exposição exacerbada do jovem, seja em termos quantitativos ou qualitativos[198]:

> Assim, parece não ser recomendável a exposição "do filho pelo filho", sem qualquer relação ou senso de pertencimento ao grupo familiar, principalmente em imagens da criança em situações vexatórias, de nudez ou seminudez que possa comprometê-la e potencializar riscos de danos. Entende-se que, essas hipóteses, há um excesso, uma abusividade na conduta dos pais.[199]

Fruto do influxo social, a superexposição dos filhos satisfaz, tão somente, a necessidade de autorrealização e de aprovação social dos pais, revelando-se em dessintonia com o melhor interesse da criança e do adolescente[200]. Em casos tais, é de se reconhecer que a tutela especial deferida ao jovem pode se estender até mesmo em face dos seus pais (art. 69, n.º 1, CRP)[201].

No ordenamento juscivilístico português, reverente Acórdão do Tribunal da Relação de Évora, de 25 de junho de 2015, impôs aos pais de uma criança de 12 anos o dever de "abster-se de divulgar fotografias ou informações que permitam identificar a filha nas redes sociais". A medida foi compreendida como "adequada e proporcional à salvaguarda do direito à reserva da intimidade da vida privada e da proteção dos dados pessoais e sobretudo da

---

tante o pedido do pai pela determinação da remoção da postagem, a Corte afirmou tratar-se de interesse legítimo da mãe "de contar, livremente, as suas histórias de vida". Por elucidativo, transcreve-se o sumário do acórdão referido: "Direito de imagem. Postagem, pela mãe, em rede social, acerca de doença de seu filho (autismo). Contrariedade do pai. Não cabimento. Embora se deva evitar a superexposição dos filhos em redes sociais, privilegiando a proteção à imagem e à intimidade do incapaz, necessário balizar tais direitos fundamentais com a liberdade de expressão da genitora. Postagem que não ofende ou desmoraliza o infante. Teor do texto publicado que demonstra preocupação e afeto com o menor. Sentença mantida. Recurso desprovido." Cf. BRASIL, Tribunal de Justiça de São Paulo, Ap. Civ. n.º. 1015089-03.2019.8.26.0577, 6ª Câmara de Direito Privado, Rel. Des. Vito Guglielmi, julgado em 13/07/2020.

[198] Ana Carolina Brochado Teixeira; Renata Vilela Multedo, *(over) Sharenting e o abuso...*, cit., p. 328.

[199] Ana Carolina Brochado Teixeira; Renata Vilela Multedo, *(over) Sharenting e o abuso...*, cit., p. 326.

[200] Segundo Brosch, uma das causas prováveis do *sharenting* é o fato de que "os pais podem se sentir validados pelas inúmeras curtidas e comentários que recebem" nas fotos de seus filhos. Sua afirmação é amparada pelo resultado de pesquisa que conduziu, em 2015, entre pais poloneses usuários do *Facebook*, a qual demonstrou que, "de um modo geral, o número de amigos [no *Facebook*] determina o número de fotos compartilhadas" [tradução livre], *vide* Anna Brosch, *When the Child...*, cit., p. 232-233.

[201] O art. 69.º, n.º 1, da Constituição da República consagra expressamente que as crianças têm direito à proteção contra o exercício abusivo da autoridade na família.

segurança da menor no Ciberespaço" face ao direito de liberdade de expressão dos progenitores.[202/203]

5. OS INSTRUMENTOS JUSCIVILISTAS DE PROTEÇÃO DA CRIANÇA/JOVEM PERANTE O *SHARENTING*

O fenômeno do *sharenting* demanda mecanismos de solução para os casos concretos, sendo necessário encontrar uma justa medida para preservar, tanto quanto possível, o direito à liberdade de expressão dos pais, sem descuidar dos direitos de personalidade das crianças e dos adolescentes e do adequado exercício das responsabilidades parentais.

Entendemos que, dificilmente, conseguir-se-á encontrar uma resposta adequada de maneira apriorística. Em virtude do valor dos direitos postos, apenas equacionando-se as circunstâncias concretas será possível chegar à melhor resolução para a problemática do compartilhamento de informações dos filhos pelos pais. Nesse capítulo, teceremos ponderações acerca de três institutos que, ao que nos parece, devem ser, especialmente, considerados.

5.1. A PROTEÇÃO DE DADOS PESSOAIS DA CRIANÇA/JOVEM EM UMA GERAÇÃO HIPERCONECTADA: A IMPORTÂNCIA DO CONSENTIMENTO NA PERSPECTIVA DO RGPD E O DIREITO AO ESQUECIMENTO APLICADO ÀS NOVAS TECNOLOGIAS ("ESQUECIMENTO DIGITAL")

A democratização dos riscos à privacidade com a utilização da informática[204] evidenciou, mais do que nunca, ser "imperioso regular o acesso, o

---

[202] Acórdão do Tribunal da Relação de Évora de 25/06/2015 (Relator: Bernardo Domingos), processo n.º 789/13.7TMSTB-B.E1, disponível em <URL: http://www.dgsi.pt/>.

[203] Miranda Barbosa considerou ter sido "excessiva a determinação judicial", eis que pautada na prospecção abstrata de um risco, qual seja o risco de exposição da criança a predadores sexuais e pedófilos, sem considerar que, no caso concreto, a extrapolação do "risco socialmente aceitável" pode não se verificar. Consoante expõe, a ilicitude do comportamento dos progenitores na divulgação de fotografias e dados da criança nas redes sociais deve "ser aferida em função de duas coordenadas: o grau de maturidade/autonomia da filha e a existência ou não de oposição desta em relação ao comportamento dos pais, por um lado; e por outro lado, o interesse do menor, pelo qual a atuação dos titulares do poder parental se terá de reger sempre". Cf. Mafalda Miranda Barbosa, "Podem os pais publicar fotografias dos filhos menores nas redes sociais? Acórdão do Tribunal da Relação de Évora, 25 de junho de 2015" *in AB Instantia – Revista do Instituto do Conhecimento AB*, Ano III, n.º 5. Coimbra, Almedina, 2015, cit., p. 313-339.

[204] "Se antes o problema era fazer face à concentração de informações nas mãos do Estado, hoje, qualquer cidadão pode, pela articulação de diversos sistemas de informação, traçar um perfil completo de outra pessoa, das suas características, dos seus bens, crenças, história clínica, aspetos da vida privada etc.". Cf. Mafalda Miranda Barbosa, "Proteção de dados e direitos de personalidade: uma relação de interioridade constituti-

tratamento e a transmissão de dados pessoais"[205], que constituem, verdadeiramente, "emanações ou extensões da personalidade"[206].

Em Portugal, o art. 35.º da Constituição consagra um direito à autodeterminação informativa que tem por finalidade, como ensinam Jorge Mirada e Rui Medeiros, "evitar intromissões abusivas na vida privada das pessoas através da recolha e tratamento de dados pessoais informatizados"[207]. O legislador constituinte impõe, ademais, uma prestação normativa ao Estado, estabelecendo que a "a tutela dos cidadãos relativamente à utilização da informática e o conteúdo dos seus direitos será definido pela lei e nos termos da lei"[208].

Essa "imposição legiferante"[209] materializa-se, no momento presente, na Lei n.º 58/2019, de 8 de agosto, que assegura a transposição, para ordem jurídica interna, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD).

Da proteção que é dispensada ao titular dos dados pessoais à luz do ordenamento jurídico vigente, para o propósito da presente tese, cumpre sublinhar a atenção que é conferida ao consentimento, principalmente no que diz respeito às crianças, as quais o RGPD enxerga como pessoas vulneráveis[210].

A proteção de dados assume estrutura procedimental de garantia, exteriorizando-se como uma forma de concretização de vários direitos de personalidade, em particular dos direitos à autodeterminação informacional, à identidade e à privacidade[211]. Por esse motivo, o consentimento, "que corporiza a autonomia"[212], assume um papel de especial relevância, enquanto

va. Os beneficiários da proteção e a responsabilidade civil" *in AB Instantia – Revista do Instituto do Conhecimento AB*, Ano V, n.º 7, Coimbra, Almedina, 2017, cit., p. 14.

205 Mafalda Miranda Barbosa, *Proteção de dados...*, cit., p. 14.

206 Inês Camarinha Lopes, "O consentimento como fundamento de licitude do tratamento de dados pessoais e o privacy paradox" *in O Sentir do Direito: Estudos em Homenagem ao Professor José Tavares de Sousa*; coordenação de André Lamas Leira, Fernando da Silva Pereira, Tiago Azevedo Ramalho, Lisboa, AAFDL – Associação Académica da Faculdade de Direito de Lisboa, 2022, cit., p. 198.

207 Jorge Miranda; Rui Medeiros, *Constituição Portuguesa anotada...*, cit., p. 785.

208 Jorge Miranda; Rui Medeiros, *Constituição Portuguesa anotada...*, cit., p. 790.

209 Para utilizar a expressão de Jorge de Miranda e Rui Medeiros. Cf. JORGE MIRANDA; Rui Medeiros, *Constituição Portuguesa anotada...*, cit., p. 790.

210 Cf. Considerando n.º 75 do RGPD. Outrossim, consta do considerando n.º 38 do RGPD que "as crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais". Inês Camarinha Lopes considera que, sem embargo do Regulamento não distinguir expressamente os sujeitos menores de idade como pertencentes a uma categorial especial de titulares de dados, pode-se considerá-los desse modo "dada a sua imaturidade e vulnerabilidade". Cf. Inês Camarinha Lopes, *Os Dados Sensíveis dos Menores à Luz do RGPD*, Coimbra, GESTLEGAL, 1.ª. ed., 2021, cit., p. 104 (nota nº. 169).

211 Alexandre Sousa Pinheiro, *Privacy e proteção...*, cit., p. 805; Mafalda Miranda Barbosa, *Proteção de dados...*, cit., p. 32.

212 Mafalda Miranda Barbosa, *Proteção de dados...*, cit., p. 28.

"principal causa de legitimidade e de licitude do tratamento de dados pessoais"[213] (art. 6º/1, *a)*, RGPD).

Atento à dimensão positiva do direito à autodeterminação informacional, relativa ao poder de supervisionar as informações pessoais eventualmente reveladas[214], o legislador comunitário enfatizou ser o consentimento livremente revogável a todo tempo[215] (art. 7º/3, RGPD)[216]. Essa previsão alcança substância por meio do direito ao apagamento dos dados, albergado no art. 17º do Regulamento, sob a alcunha "direito a ser esquecido"[217].

Nos termos do RGPD, "o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada", quando, *inter alia*, o consentimento em que se baseia esse tratamento tenha sido retirado (art. 17.º/1, *b)*, RGPD)[218].

---

[213] António Barreto Menezes Cordeiro, *Direito da proteção de dados: à luz do RGPD e da Lei n.º 58/2019*, 1ª ed., Coimbra, Almedina, 2020, cit., p. 167. Em igual sentido, Mafalda Miranda Barbosa, *Proteção de dados...*, cit., p. 27.

[214] Jorge Miranda; Rui Medeiros, *Constituição Portuguesa anotada...*, cit., p. 789.

[215] Inês Camarinha Lopes ressalta que o direito à retirada do consentimento prestado constitui verdadeiro direito potestativo do titular de dados, consagrado em ordem a respeitar a sua autonomia. Cf. Inês Camarinha Lopes, *O consentimento...*, cit., p. 201 e p. 205.

[216] As condições aplicáveis ao consentimento estão previstas no art. 7.º do RGPD, tendo o legislador comunitário discernido a necessidade de acautelar especificamente as crianças em relação à oferta direta de serviços da sociedade da informação, dada a sua situação de especial vulnerabilidade. Pese embora esteja o regime singular estabelecido pelo art. 8.º do RGPD restrito à oferta direta de serviços, não nos cabendo delinear os seus parâmetros no presente estudo, a previsão de norma destinada expressamente às crianças denota a preocupação do sistema jurídico com à proteção dos sujeitos menores de idade, o que não se pode desconsiderar. Sobre uma análise detida acerca do alcance do art. 8.º do Regulamento, *vide* Inês Camarinha Lopes, *Os Dados Sensíveis...*, cit., p. 103 e ss.

[217] Caso emblemático no que se refere ao direito ao esquecimento se deu sob a égide da Diretiva 95/46/CE. Tratou-se de situação que dizia respeito "à exibição, na lista de resultados que o internauta obtém ao efetuar no Google Search uma pesquisa a partir do nome da pessoa em causa, de ligações a páginas de arquivos em linha de um jornal que contém anúncios que mencionam o nome dessa pessoa e que respeitam a uma venda de imóveis em hasta pública decorrente de um arresto com vista à recuperação de dívidas à Segurança Social". Na oportunidade, o Tribunal de Justiça da União Europeia ponderou que o motor de busca era obrigado a suprimir as referidas ligações da lista de resultados, argumentando ser necessário "considerar que, tendo em conta o caráter sensível, para a vida privada dessa pessoa, das informações contidas nesses anúncios e o facto de a sua publicação inicial remontar há 16 anos, a pessoa em causa tem comprovadamente direito a que essas informações já não sejam associadas ao seu nome através dessa lista". Cf. União Europeia, Tribunal de Justiça da União Europeia, Grande Secção, Acórdão de 13/05/2014, processo nº C-131/12, Google Spain SL, Google Inc. contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González, disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9959369.

[218] Maria Raquel Guimarães aponta as dificuldades técnicas na salvaguarda deste direito, "na medida em que uma vez difundida uma informação *on-line* ela pode ser repro-

Esse direito ao "esquecimento digital" se relaciona, fundamentalmente, "com a criação e a manutenção de um nível razoável de privacidade informacional"[219] diante do potencial de perpetuidade assumido pela informação lançada na *Internet*[220].

No caso do *sharenting*, as plataformas em linha, designadamente as redes sociais, funcionam como intermediários para divulgação dos dados pessoais da criança ou do jovem pelos seus pais[221]. Ao efetuar uma atividade de armazenamento de dados[222/223], também a elas recai a obrigação de facultar ao titular o direito de apagamento de suas informações, o que inclui, incontestavelmente, as situações em que, atingida a maioridade, o titular retire o consentimento fornecido pelo então representante legal quanto a imagens e outros elementos que tenham sido coletados durante a sua infância.

Para Steinberg, o direito ao esquecimento pode se revelar como a solução legal mais promissora para remediar os danos causados pela divulgação *online* de informações pessoais de uma criança pelos seus pais. Segundo propõe, não só após atingida a maioridade deve poder ser exercido o direito

---

duzida sucessivamente, retirando eficácia prática a uma ordem imposta para a 'apagar' no servidor onde foi primeiramente alojada". Cf. Maria Raquel Guimarães, *A Tutela da Pessoa...*, cit., p. 31.

219 Hans Graux; Jef Ausloos; Peggy Valcke, "The right to be forgotten in the internet era" *in ICRI Research Paper*, n.º 11, 2012, disponível em https://ssrn.com/abstract=2174896. (25.06.2022), cit., p. 5.

220 "O ser humano tende a esquecer determinados detalhes e a dar um novo significado às experiências vividas com o decurso do tempo, o que não é possível pela estaticidade da informação veiculada na rede, que, ao ser retomada, pode impedir ou dificultar esse processo de ressignificação". Cf Lívia Teixeira Leal, *O Cuidado na era digital...*, cit., p. 272.

221 Fernando Büscher Von Teschenhausen Eberlin, *Sharenting, liberdade de expressão...*, cit., p. 264.

222 David Erdos classifica as redes sociais como *controller hosts*, tendo em vista que essas plataformas não só possibilitam a publicação pelos usuários, mas determinam a forma como as informações publicadas serão comunicadas a terceiros, combinado e alinhando conteúdos ou sugerindo sua visualização para determinados usuários. Cf. David Erdos, "Intermediary publishers and European data protection: Delimiting the ambit of responsibility for third-party rights through a synthetic interpretation of the EU acquis" *in International Journal of Technology*, Vol. 26, n.º 3, 2018, disponível em https://academic.oup.com/ijlit/article/26/3/189/5033541 (30.06.2022), cit., p. 214.

223 Em março de 2022 foi alcançado acordo político entre o Parlamento Europeu e os Estados-Membros da UE quanto à proposta de regulamento sobre os serviços digitais (RSD), apresentada pela Comissão Europeia em dezembro de 2020. O acordo alcançado está sujeito à aprovação formal dos dois colegisladores e, uma vez adotado, será aplicável em toda a União Europeia quinze meses após a sua entrada em vigor ou a partir de 1 de janeiro de 2024, conforme o que ocorrer mais tarde. A exposição de motivos do RSD reconhece as redes sociais como prestadoras de serviços intermediários, lendo-se no considerando 13 que "as plataformas em linha, como as redes sociais ou os mercados em linha, devem ser definidas como prestadores de serviços de armazenagem em servidor que não só armazenam informações fornecidas pelos destinatários do serviço a pedido dos mesmos, mas também divulgam essas informações ao público, mais uma vez a pedido dos mesmos".

ao esquecimento pelos sujeitos menores de idade, carecendo ser levada em consideração a efetiva capacidade do jovem para consentir:

> O direito ao esquecimento reconhece que, com o passar do tempo, o valor da divulgação é minimizado e deve dar lugar aos interesses concorrentes de privacidade da criança. Quando um pai compartilha informações sobre uma criança online, o propósito expressivo da divulgação diminui à medida que a criança envelhece. O direito ao esquecimento permite aos pais a liberdade de falar sobre seus filhos nas redes sociais e blogs. Também não infringe o direito dos pais de expressar livremente suas opiniões sobre a paternidade e permite que os pais controlem a divulgação de informações sobre a criança como membro da unidade familiar. Além disso, apoia o direito dos pais à liberdade de expressão. [...] Ao utilizar políticas como o direito ao esquecimento, os tribunais podem reconhecer que as crianças têm uma capacidade crescente de fornecer consentimento. De acordo com essa teoria, os tribunais podem sustentar que crianças pequenas consentem indiretamente com as revelações dos pais, mas à medida que as crianças crescem, elas devem ter mais controle sobre suas informações pessoais. [tradução livre][224]

A posição adotada por Steinberg se coaduna com a visão moderna da criança e do adolescente como seres em desenvolvimento, cujas capacidades e maturidade adquirem contornos diferenciados nas sucessivas etapas da vida[225]. Ressalte-se, por esse ângulo, que o RGPD reconhece, *a contrario sensu*, a capacidade do sujeito de 16 anos para consentir no que respeita à oferta direta de serviços da sociedade da informação (art. 8.º/1), limite etário que é reduzido pelo direito interno português para 13 anos (art. 16º, n.º 2, Lei n.º 58/2019).

5.2. A EVENTUAL RESPONSABILIZAÇÃO CIVIL DOS PROGENITORES

Apesar de a família ser reconhecida como "instituição que extravasa o mundo do juridicamente relevante", exige-se do direito uma resposta "adequada à sua própria intencionalidade"[226]. Discute-se, nesses termos, em que medida a responsabilidade civil se aplica às relações familiares.

Tradicionalmente, chamava-se à colação a ideia de fragilidade da garantia dos direitos familiares pessoais, segundo a qual o caráter extremamente íntimo desses direitos tornaria impossível "forçar, externamente, a sua observância"[227]. A tutela predisposta para os direitos familiares de natureza

---

224 Stacey B. Steinberg, *Sharenting: Children's Privacy...*, cit., p. 876.

225 A esse respeito, veja-se o capítulo primeiro da presente tese (tópico 2), em particular o item "b" do tópico 2.2.

226 Mafalda Miranda Barbosa, "Família e responsabilidade civil: uma relação possível? Brevíssimo apontamento" *in Lex Familiae – Revista Portuguesa de Direito de Família*, Ano 10, n.º 20, Coimbra Editora, jul./dez. 2013, cit., p. 62.

227 Cristina Manuela Araújo Dias, "Responsabilidade civil e direitos familiares conjugais (pessoais e patrimoniais): possibilidade de indemnização ou fragilidade da garantia?" *in Scientia Ivridica – Revista de Direito Comparado Português e Brasileiro,* n.º 286/288, 2000, cit., p. 357. Particularmente no que diz respeito à relação entre pais e filhos, a re-

pessoal seria, assim, "de outra ordem"[228], notadamente através de institutos próprios do direito de família[229].

Nada obstante, sobretudo desde a segunda metade do séc. XX, observou-se uma "tendência de retraimento"[230] dos sistemas jurídicos na regulação da intimidade no âmbito das famílias, em face do "pluralismo social que se instalou duradouramente nas comunidades ocidentais"[231] e que se opôs a estrutura patriarcal então vigente. Afora o valor supraindividual do grupo familiar, percebeu-se a família como ambiente de afirmação dos direitos de personalidade dos seus integrantes, bem como de realização das suas aspirações individuais e do seu modo de ser[232].

À vista disso, e particularmente após a reforma de 2008, introduzida pela Lei n.º 61/2008, de 31 de outubro[233], vem-se "aceitando, doutrinal e jurisprudencialmente, a derrocada da tradicional 'fragilidade da garantia' dos direitos familiares pessoais"[234] e o cabimento da tutela ressarcitória, através da

posta negativa à pretensão indenizatória assentava-se na chamada "imunidade parental", suportada nas ideais da paz da família e da tranquilidade da vida social. Cf. Guilherme De Oliveira, "Responsabilidade civil dos pais perante os filhos" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 18, n.º 35, Coimbra Editora, 2021, cit., p. 5.

228 João De Matos Antunes Varela, *Das obrigações em geral*, Vol. I, 10.ª. ed., Coimbra, Almedina, 2000, cit., p. 535.

229 "Seriam, portanto, a limitação ou a inibição total ou parcial do exercício das responsabilidades parentais, a aplicação de medidas de promoção e proteção ditadas pela LPPCJP, a incapacidade sucessória, etc." Cf. Guilherme De Oliveira, *Responsabilidade civil dos pais...*, cit., p. 9.

230 Guilherme De Oliveira, "Responsabilidade civil por violação dos deveres conjugais" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 16, n.º 31-32, Coimbra Editora, 2019, cit., p. 33.

231 Guilherme De Oliveira, *Responsabilidade civil por violação...*, cit., p. 22.

232 Sobre transformação da família a partir da emergência do paradigma personalista, veja-se Rute Teixeira Pedro, *A visão personalista...*

233 Guilherme De Oliveira, *Responsabilidade civil por violação...*, cit., p. 33; Jorge Ribeiro De Faria, *Direito das obrigações*, volume I, 2ª ed. atualizada e ampliada por Miguel Pestana de Vasconcelos e Rute Teixeira Pedro, Coimbra, Almedina, 2020, cit., p. 409.

234 Jorge Ribeiro De Faria, *Direito das obrigações...*, cit., p. 409. Em igual sentido, Heinrich Ewald Hörster, "A responsabilidade civil entre os cônjuges" *in E foram felizes para sempre...? Uma análise crítica do novo regime jurídico do divórcio. Actas do Congresso de 23, 24 e 25 de outubro de 2008*; coordenação de Maria Clara Sottomayor, Maria Teresa Féria de Almeida, Wolters Kluwer Portugal, Coimbra, Coimbra Editora, 2010, cit., p. 109; e Rute Teixeira Pedro, "A responsabilidade Civil como (derradeira) manifestação de juridicidade dos deveres conjugais? Anotação ao Acórdão do Supremo Tribunal de Justiça (2.ª Secção) de 12.5.2016, Proc. 2325/12.3TVLSB.L1.S1" *in Cadernos de Direito Privado*, n.º 61, janeiro/março de 2018, cit., p. 57.

responsabilidade civil, em hipóteses de violação desses direitos[235], dentre os quais se inserem as responsabilidades parentais[236].

Especificamente no que toca às relações entre pais e filhos, Guilherme de Oliveira destaca que o seio familiar não pode ser um terreno livre de não-direito, onde as ofensas causadas aos direitos de personalidade do jovem ficam por apreciar e reparar, ponderando que não há no ordenamento juscivilístico português "qualquer norma que exclua a responsabilidade civil por condutas ilícitas que causem danos ao filho"[237]; e continua:

> Além disto, é bom notar que não é o sistema legal, nem os tribunais, que intentam as ações de responsabilidade dos filhos contra os pais, oficiosamente — são os filhos, por si ou por representante legal, que as promovem. É a estes autores que caberá decidir se a natureza das ações ou omissões ilícitas, os danos causados, e as condições concretas em que a família vive, justificam que se inicie o litígio. [...] O sistema tem de estar aberto para acolher as escolhas individuais no quadro de uma grande diversidade de casos; e não pode fechar hermeticamente todas as portas, para todos os casos[238].

Admitida, em abstrato, a possibilidade de pretensão indenizatória dos filhos em face dos progenitores, o que se questiona, nesse trabalho, é se a prática do *sharenting* pode configurar modalidade de responsabilidade civil em concreto exigível.

Já tivemos a oportunidade de analisar que, quando efetuado dentro de certos limites, o compartilhamento de informações pessoais dos filhos pe-

---

235 Sobre o tema, são eminentes os ensinamentos de Rute Teixeira Pedro: "[...] também no domínio da responsabilidade civil se constata a preocupação de tutela da pessoa e dos múltiplos bens (de personalidade) em que ela se desdobra. Assim, o contexto em que a mesma se integra e as relações que são entretecidas com outras pessoas e dão significado à existência individual de cada um não são ignorados para efeitos ressarcitórios. Aceita-se, de forma crescente, que as perturbações ou afetações negativas daquelas relações possam ser qualificadas como danos atendíveis merecedores de reparação, desde que todos os requisitos constitutivos da responsabilidade civil se encontrem verificados. [...] Assim, quanto aos atos que seriam ilícitos fora do contexto familiar, atentatórios de posições jurídicas não familiares (por exemplo, do direito à vida, do direito à integridade física, ...), o facto de lesante e lesado estarem ligados por um vínculo familiar – no caso conjugal – não deve ditar a exclusão do funcionamento da responsabilidade civil". Cf. Rute Teixeira Pedro, *A responsabilidade Civil como (derradeira)...*, cit., p. 61. Com igual percepção, Jorge Ribeiro De Faria, *Direito das obrigações...*, cit., p. 409; e Mafalda Miranda Barbosa, *Família e responsabilidade civil...*, cit., p. 69. Exemplificativamente, cita-se, ainda, o Acórdão do Tribunal da Relação de Lisboa de 07/10/2021 (Relator: Jorge Leal), processo n.º 58/20.6T8SCG.L1-2, disponível em <URL: http://www.dgsi.pt/>, cujo sumário se fez nos seguintes termos: "A responsabilidade civil emergente da violação de direitos de personalidade pode fundar a instauração de ação de indemnização por danos não patrimoniais de um cônjuge contra o outro, a deduzir nos tribunais comuns".

236 Francisco Pereira Coelho; Guilherme De Oliveira, *Curso de Direito da Família...*, cit., p. 180.

237 Guilherme De Oliveira, *Responsabilidade civil dos pais...*, cit., p. 9.

238 Guilherme De Oliveira, *Responsabilidade civil dos pais...*, cit., p. 10.

los pais reflete o direito à liberdade de expressão desses últimos, bem como se mostra consentâneo com a autonomia dos progenitores no exercício das responsabilidades parentais[239].

Se quando realizado de forma módica, o *sharenting* encontra respaldo na nossa ordem jurídica, o mesmo não acontece quando os pais ultrapassam os espaços de liberdade e agem de forma excessiva. A atuação descomedida dos pais nas redes sociais se afasta do princípio motor do cuidado parental, qual seja o interesse da criança e do adolescente, sobrepondo a vontade dos pais à preservação da saúde mental e da integridade emocional do filho, em verdadeiro exercício disfuncional das responsabilidades parentais.

Ora, a preterição dos deveres inerentes ao conteúdo das responsabilidades parentais outra coisa não é senão o exercício abusivo da posição jurídica ocupada pelos progenitores[240], pelo que a conduta dos pais se mostra passível de responsabilização, atraindo a disciplina do abuso de direito (art. 334.º, CC)[241]:

> Se o artigo 334.º permite sindicar o exercício de um direito que não está funcionalizado, atendendo à boa-fé, aos bons costumes e ao fim económico e social desse direito, por maioria de razão deve ser sindicado o exercício do poder paternal. [...] Ora, ainda que o poder funcional não se possa ser qualificado como direito subjectivo, estamos diante de uma posição subjectiva activa, funcionalizada no seu exercício à salvaguarda do interesse do menor, donde o exercício desse poder que olvide a finalidade que lhe preside e ponha em causa o interesse do menor deve ser considerado abusivo. Pelo que, ainda que não viole direitos dotados de eficácia absoluta de que o filho seja titular, o comportamento do pai pode fundar uma pretensão indemnizatória pelos da-

---

239 Veja-se o tópico 4.3.

240 Ana Carolina Brochado Teixeira; Renata Vilela Multedo, "A responsabilidade dos pais pela exposição excessiva dos filhos menores nas redes sociais: o fenômeno do sharenting" *in Responsabilidade Civil e Direito de Família: O Direito de Danos na Parentalidade e Conjugalidade*, Ana Carla Harmatiuk Matos [Et Al], Indaiatuba, Editora Foco, 2021, cit., p. 15-16. Em outra oportunidade, TEIXEIRA e MULTEDO se posicionaram no sentido de que não haveria, tecnicamente, abuso de direito no exercício das responsabilidades parentais, mas sim no exercício do direito à liberdade de expressão dos pais, *vide* Ana Carolina Brochado Teixeira; Renata Vilela Multedo, *(over)Sharenting e o abuso...*, cit., p. 331 (nota n.º 46). Não é esse o entendimento adotado nesse estudo. Percebemos que o exercício abusivo da liberdade de expressão pelos pais acarreta abuso de direito no exercício das responsabilidades parentais, desviando-o de sua finalidade intrínseca, que é o cuidado com a criança e a promoção do seu desenvolvimento saudável.

241 Comentando a previsão legal de abuso de direito no Código Civil, Menezes Cordeiro sublinha que "a locução 'direito' surge, aqui, numa acepção muito ampla, de modo a abranger o exercício de quaisquer posições jurídicas, incluindo as passivas". Segundo Cordeiro, de 2001 em diante, o instituto do abuso do direito desligou-se da ideia de direito subjetivo, configurando-se "como uma instância geral de controlo dos exercícios jurídicos". Cf. António Menezes Cordeiro, "Do abuso do direito: estado das questões e perspectivas" in Revista da Ordem dos Advogados (ROA), Ano 65, Vol. II, Set. 2005, disponível em https://portal.oa.pt/publicacoes/revista-da-ordem-dos-advogados-roa/ano-2005/ano-65-vol-ii-set-2005/artigos-doutrinais/antonio-menezes-cordeiro-do-abuso-do-direito-estado-das-questoes-e-perspectivas-star/# (23.06.2022), cit., s/p.

> nos causados, na medida em que o exercício abusivo a que assim fazemos referência corresponde a uma prática que viola a dimensão de autonomia do ser pessoa (do menor) e a sua dignidade como pessoa.[242]

Caracterizada a ilicitude do *oversharenting*, a obrigação de indenizar se fará impor uma vez observados os demais requisitos do art. 483.º, CC[243], devendo, por óbvio, ser abrangidos os danos não patrimoniais[244] resultantes da ofensa à personalidade da criança ou adolescente (art. 496.º, CC)[245/246].

Importa, no entanto, fazer uma advertência. Como alerta Carneiro da Frada, "jamais a proteção jurídica pode ir tão longe que pretenda eliminar o risco geral da vida e constranger, mais do que o razoável, a autonomia e a liberdade dos sujeitos"[247]. Quer isto dizer que admitir o recurso à responsabilidade civil não pode significar uma completa descaracterização da rela-

---

242 Mafalda Miranda Barbosa, *Família e responsabilidade civil...*, cit., p. 75-76.

243 "[...] à face dele [art. 483.º, CC] incorre em responsabilidade, e portanto numa obrigação de indemnizar, quem pratica um facto voluntário (é a 'Handlung' dos alemães), que traduza ou incorpore um juízo de desvalor objetivo da ordem jurídica ('Rechtswidrigkeit'), sendo o seu agente censurável ('Verschuldengrundsatz'), ponto é que tenham ocorrido danos que se ligam causalmente àquele facto. Quer dizer, para haver uma obrigação de indemnizar é preciso: 1. um facto voluntário; 2. a ilicitude; 3. a culpa; 4. o dano; 5. o nexo de causalidade ente o facto e o dano." Cf. Jorge Ribeiro De Faria, *Direito das obrigações...*, cit., p. 406.

244 Rute Teixeira Pedro destaca a erosão de barreiras tradicionais associadas ao instituto da responsabilidade civil e "uma ampliação crescente das soluções compensatórias de danos não patrimoniais", que revelam, nos planos doutrinal, jurisprudencial e legal, "a emergência de uma conceção integral e relacional da pessoa, aglutinadora das múltiplas dimensões (sob o ponto de vista anatómico, funcional, estético e emocional, por exemplo) em que a mesma se desdobra e das variadas potencialidades que a mesma encerra e se desenvolvem, numa perspetiva dinâmica, através de atividades variadas e de laços entretecidos com outros pessoas, e mesmo com animais e coisas". Cf. Rute Teixeira Pedro, "Da ressarcibilidade dos danos não patrimoniais no direito português: a emergência de uma nova expressão compensatória da pessoa – Reflexão por ocasião do quinquagésimo aniversário do Código Civil*" in Estudos Comemorativos dos 20 anos da FDUP*, Vol. II, Coimbra, Almedina, 2017, cit., p. 710-711.

245 Nos termos do art. 496.º, n.º 1, do Código Civil, para serem compensáveis, os danos não patrimoniais devem merecer a tutela do direito, o que "importa um juízo sobre a gravidade do dano produzido". Cf. Rute Teixeira Pedro, "Os danos não patrimoniais (ditos) indiretos: uma reflexão ratione personae sobre a sua ressarcibilidade" *in Responsabilidade Civil: cinquenta anos em Portugal, quinze anos no Brasil*; coordenação de Mafalda Miranda Barbosa, Francisco Muniz, Coimbra, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, 2017, cit., p. 249. Assim também, Heinrich Ewald Hörster, *A responsabilidade civil...*, cit., p. 109.

246 Segundo Guilherme de Oliveira, uma vez admitido o recurso à responsabilidade civil, diversos motivos são idôneos para fundamentar um pedido de indenização, dentre os quais a exposição pelos pais da "imagem de um filho, sem o seu consentimento, em redes sociais ou em programas televisivos", *vide* Guilherme De Oliveira, *Responsabilidade civil dos pais...*, cit., p. 14.

247 Manuel A. Carneiro Da Frada, "Nos 40 anos do Código Civil Português: tutela da personalidade e dano existencial" *in Themis, Revista de Direito*, Edição Especial, Lisboa, Faculdade de Direito da Universidade Nova de Lisboa, 2008, cit., p. 193.

ção entre pais e filhos, sendo pertinente avaliar, *in concreto*, se não há outra medida capaz de salvaguardar, satisfatoriamente, os interesses do sujeito menor de idade[248].

Entre nós, "a proteção da pessoa está omnipresente no direito civil"[249], reconhecendo-se ampla tutela à personalidade nos termos do art. 70.º, CC[250]. Desse modo, oportuniza-se a adoção de remédios diretos destinados a prevenir ou a reduzir os efeitos de eventual ofensa[251] (art. 878.º, do Código de Processo Civil), que, igualmente, devem ser considerados nos casos de *sharenting*[252].

Essa parece ser a solução mais razoável, estando, inclusive, em consonância com o entendimento do Supremo Tribunal de Justiça, segundo o qual "a aplicação do instituto do abuso do direito tem uma natureza subsidiária, só a ele sendo lícito recorrer na falta de uma norma jurídica que resolva, de forma adequada, a questão em causa"[253].

Deve-se, portanto, a partir das circunstâncias do caso *sub judice*, ponderar o grau de ilicitude da conduta[254] dos pais, bem como a extensão dos

---

248 "Admito que, num território delicado como o das relações entre pais e filhos, talvez seja recomendável que o sistema encontre um caminho capaz de conciliar os interesses, praticando algumas intervenções preventivas — com o sentido de diminuir a conflitualidade e fomentar a restauração das relações em crise — de tal modo que o recurso à responsabilidade civil possa constituir um último remédio. Penso nas intervenções destinadas à tutela da personalidade, previstas no art. 878.º CProcCiv, na aplicação dos arts. 3.º e 35.º da LPCJP, nas medidas tutelares cíveis" Cf. Guilherme De Oliveira, *Responsabilidade civil dos pais...*, cit., p. 12.

249 Manuel A. Carneiro Da Frada, *Nos 40 anos do Código Civil Português...*, cit., p. 188. De igual modo, Rute Teixeira Pedro: "A previsão de direitos especiais de personalidade e o reconhecimento de um 'direito geral de personalidade', no plano civilístico (art.º 70.º do CC) e a consagração de um direito ao livre desenvolvimento da personalidade, no plano constitucional (art.º 26.º CRP), proporcionam uma tutela 'vocacionadamente globalizante e, por isso, tendencialmente contínua'. Do mesmo passo a proteção dos bens pessoais é impregnada de uma perspetiva dinâmica e evolutiva, aberta ao florescimento dos atributos da pessoa." Cf. Rute Teixeira Pedro, *Da ressarcibilidade dos danos...*, cit., p. 703.

250 "O direito geral de personalidade [...] não é um mero suprimento da escassez dos direitos de personalidade especiais, nem uma súmula desses direitos, mas o direito-matriz ou fundante de todas essas emergências na lei, o que lhes dá o verdadeiro sentido e a cuja luz todas devem ser interpretadas. É a expressão do domínio de si que a persona constitui antes de tudo." Cf. Orlando De Carvalho, *Teoria Geral...*, cit., p. 263.

251 Pedro Pais De Vasconcelos, *Direito de Personalidade*, Coimbra, Almedina, 2006, cit., p. 127 e ss.

252 Não se pode deixar de citar, mais uma vez, o Acórdão do Tribunal da Relação de Évora de 25/06/2015 proferido no âmbito de um processo de regulação do exercício das responsabilidades parentais, que impôs aos pais o dever de abstenção quanto à divulgação de fotografias e informações da filha nas redes sociais. Sobre a decisão, *vide* ponto. 3.3 do presente estudo.

253 Acórdão do Supremo Tribunal de Justiça de 16/11/2021 (Relatora: Maria Clara Sottomayor), processo n.º 21827/17.9T8SNT-A.L1.L1.S1, disponível em <URL: http://www.dgsi.pt/>.

254 "Para a apreciação do grau de ilicitude deve ainda ser ajuizado, em concreto, o modo como foi feita a publicitação da imagem ou a revelação dos factos da vida privada. Ensina a prática que há muitas maneiras de revelar a imagem ou a vida privada das pessoas. Pode ser

danos causados aos direitos de personalidade da criança ou do adolescente e a efetividade da medida a ser adotada na proteção dos seus interesses.

5.3. A INIBIÇÃO AO EXERCÍCIO DAS RESPONSABILIDADES PARENTAIS

O exercício das responsabilidades parentais está sujeito à vigilância do Estado[255], dada a proteção dispensada, pela ordem jurídica, à infância e ao direito ao desenvolvimento da personalidade das crianças e dos adolescentes.

Nesse sentido, a Constituição da República prevê, expressamente, que à criança é assegurada proteção contra o exercício abusivo da autoridade na família (art. 69.º, n.º 1), motivo pelo qual, em situações de grave "incumprimento ou cumprimento defeituoso das responsabilidades parentais"[256], admitem-se restrições ao princípio de que os filhos não podem ser separados dos pais (art. 36.º, n.º 6)[257].

A seriedade da medida de inibição do exercício das responsabilidades parentais (art. 1915.º, CC) dita, todavia, que essa intervenção restritiva seja submetida "a um rigoroso crivo de proporcionalidade"[258], o que exige seja decretada, tão somente, quando não existirem soluções menos gravosas passíveis de acautelar o superior interesse da criança[259].

Diante da carência no cumprimento dos poderes-deveres inerentes ao cuidado parental presente nas situações de *oversharenting*[260] pensamos

feita de modos mais ou menos ofensivos ou vexatórios, ou mesmo de modos inocentes ou inócuos." Cf. PEDRO PAIS DE VASCONCELOS, *Direito de Personalidade...*, cit., p. 139.

255 Maria Clara Sottomayor, *O poder paternal...*, cit., p. 50.

256 Jorge Miranda; Rui Medeiros, *Constituição Portuguesa anotada...*, cit., p. 834.

257 "Esta garantia, que consiste em os filhos não poderem, em princípio, ser separados dos pais, não constitui apenas um direito subjectivo dos próprios pais a não serem separados dos seus filhos, mas também um direito subjectivo dos filhos a não serem separados dos respectivos pais. Eventuais restrições aos mesmos direitos apenas serão possíveis mediante decisão judicial, nos casos especialmente previstos por lei e verificados os pressupostos expressamente previstos na Constituição: quando se torne necessário salvaguardar os direitos dos menores, por os pais não cumprirem os seus deveres para com eles. Assim se pretende proteger a família, como o impõe o artigo 67º, nº 1, do texto constitucional." Cf. Acórdão do N.º 181/97 do Tribunal Constitucional de 05/03/1997 (Relator: Luís Nunes de Almeida), disponível em <URL: http://www.tribunalconstitucional.pt/tc/acordaos/19970181.html>

258 Jorge Miranda; Rui Medeiros, *Constituição Portuguesa anotada...*, cit., p. 833.

259 Havendo perigo para a segurança, a saúde, a formação moral ou a educação do filho, o Código Civil prenuncia, como alternativas à inibição das responsabilidades parentais, medidas de assistência que permitem aos pais conservar o exercício do cuidado parental em tudo o que com elas não se mostra inconciliável (art. 1918.º, CC). BOLIEIRO e GUERRA alertam que "só em casos de absoluta nitidez e conveniência do ponto de vista do interesse da criança se deve concluir que é impossível decretar as limitações previstas no art. 1918.º do CC, por ser o caso, antes, de inibição do exercício das RP". Cf. Helena Bolieiro; Paulo Guerra, *A criança...*, cit., p. 306. Em igual sentido, Helena Gomes De Melo [Et Al], *Poder paternal...*, cit., p. 170.

260 Aqui, utiliza-se a expressão *oversharenting* para indicar o exercício não moderado da prática do *sharenting*, não englobando as hipóteses corriqueiras que respeitem os limi-

que não se pode excluir, aprioristicamente, a possibilidade de decretação da medida do art. 1915.º, do CC[261], de maneira desconexa às circunstâncias do caso concreto. Apenas a análise *in casu* será apta a demonstrar se a inibição do exercício das responsabilidades parentais é, não só razoável, mas necessária para resguardar a personalidade dos filhos[262].

Nos Estados Unidos da América, um pai perdeu a guarda de dois dos seus cinco filhos após divulgar diversos vídeos na plataforma *YouTube.* O conteúdo apresentado no canal intitulado *DaddyOFive* – que continha mais de 750.000 inscritos e contava com mais de 176 milhões de visualizações – era o de "pegadinhas" com as crianças, que incluíam abuso psicológico e agressões físicas[263].

Uma tendência preocupante que se tem observado e que pode dar ensejo a discussões quanto à limitação do exercício das responsabilidades parentais é a utilização do *sharenting* como meio para disciplinar os filhos. Alguns pais estão ganhando fama na *Internet* por postaram fotos de seus filhos segurando cartazes que detalham a sua má atitude ou conduta[264], com o objetivo de alcançar uma mudança comportamental por meio da vergonha pública[265].

---

tes impostos pelo respeito à personalidade do sujeito menor de idade. Sobre os conceitos, remete-se o leitor para tópico 4 do presente estudo.

261 Para uma apreciação detida acerca da medida de inibição do exercício das responsabilidades parentais, mormente quanto à distinção da sua decretação diretamente da lei (*ope legis*) ou de decisão judicial (*ope judicis*), veja-se Jorge Duarte Pinheiro, *O Direito da Família...*, cit., p. 304 e ss.; e Maria Clara Sottomayor, *O poder paternal*..., cit., p.50 e ss.

262 Exsurge da axiologia do ordenamento que a inibição do exercício das responsabilidades parentais consiste numa medida de proteção das crianças, e não na imposição de sanção para os progenitores, inclusive no que diz respeito à "inibição de pleno direito em relação aos condenados definitivamente por crime a que a lei atribua esse efeito". Cf. Maria Clara Sottomayor, *O poder paternal*..., cit., p. 51.

263 Nos vídeos, as crianças eram submetidas a gritos, empurrões e palavras de baixo-calão pelo pai e pela madrasta, tinham seus brinquedos quebrados e apareciam chorando inconsolavelmente. Em uma das "pegadinhas", o filho mais novo foi informado que havia sido adotado por outra família. Segundo os promotores que atuaram no caso, as crianças experimentaram "danos substanciais em sua capacidade mental ou psicológica de funcionar" [tradução livre], *vide* S/A, "DaddyOFive parents lose custody 'over YouTube pranks'", *in BBC NEWS*, 2017, disponível em https://www.bbc.com/news/technology-39783670 (25/06/2022); Sam Levin, "Couple who screamed at their kids in YouTube 'prank' sentenced to probationg'", *in The Guardian*, 2017, disponível em https://www.theguardian.com/us-news/2017/sep/12/youtube-parents-children-heather-mike-martin (25/06/2022); e Mahita Gajanan, "YouTube Star DaddyOFive Loses Custody of 2 Children Shown in 'Prank' Videos", *in TIME*, 2017, disponível em https://time.com/4763981/daddyofive-mike-martin-heather-martin-youtube-prank-custody/ (25/06/2022).

264 Stacey B. Steinberg, *Sharenting: Children's Privacy...*, cit., p. 853-854.

265 "A vergonha como forma de punição comportamental para crianças existe há milhares de anos. Mas, em um mundo cada vez mais *online*, redes sociais como *Youtube* e *Facebook* deram aos pais novos ambientes para envergonhar o mau comportamento de seus filhos. Esses espaços são, inevitavelmente, mais visíveis e amplificados, e os efeitos são, portanto, mais nocivos e permanentes...Do ponto de vista do neurodesenvolvimento, as estruturas sociais do cérebro são críticas para o desenvolvimento de um adolescente, e é por

Trazendo essa factualidade para a nossa ordem jurídica, é de se questionar se casos tais não são passíveis de ensejar a inibição no exercício do cuidado parental ou, ao menos, a adoção de providência albergada no art. 1918.º, do CC[266], sendo certo que o direito de os pais educarem os filhos não abrange o direito de agredirem sua dignidade e integridade psíquica[267]. Explica-nos Maria Clara Sottomayor:

> O direito a métodos educativos e de disciplina não violentos e não humilhantes, apesar de não estar expressamente previsto na lei civil, resulta de uma interpretação sistemática dos artigos 69.º, n.º 1 da CRP (direito à protecção da sociedade e doestado contra abusos de autoridade) e do art. 1878.º (conteúdo das responsabilidades parentais), em consonância com os arts 152.º, n.º 1 e 152.º A, n.º 1, al. a) do CP, que tipificam, como crimes de violência doméstica e de maus tratos, os castigos corporais a crianças, trabalhadores ou outros dependentes.[268]

O compartilhamento de informações pessoais dos filhos menores de idade pelos pais pode se revestir de diferentes características e a resposta do direito precisa ser ajustada à ofensa concretamente perpetrada. Se é verdade que a inibição do exercício das responsabilidades parentais assume a qualidade de *ultima ratio*[269], não é menos verdade que o quadro fático pode se mostrar de tal magnitude que exija essa medida.

---

isso que muitos adolescentes são mais sensíveis à avaliação social de seus pares...A adolescência não é apenas uma época em que grandes mudanças no desenvolvimento neurológico estão afetando as suas funções executivas, é uma época em que os adolescentes estão tentando estabelecer suas próprias identidades e independência de seus pais." [tradução livre]. Cf. Valentin & Blackstock Psychol, The Dark Side of Public Shaming Parenting *Apud* Stacey B. Steinberg, *Sharenting: Children's Privacy...*, cit., p. 854 (nota n.º 97).

266 Recorda-se que, nos termos do art. 3.º, n.º 2, al. b), c) e f) da Lei 147/99, de 1 de setembro, as crianças ou jovens que sofram maus tratos físicos ou psíquicos, não recebam os cuidados adequados ou estejam sujeitos a comportamentos que afetem gravemente o seu equilíbrio emocional são consideradas "em perigo".

267 Maria Clara Sottomayor, *O poder paternal*..., cit., p. 48.

268 Maria Clara Sottomayor, "A autonomia do direito das crianças" *in Estudos em Homenagem a Rui Epifânio*; coordenação de Armando Leandro, Álvaro Laborinho Lúcio, Paulo Guerra, Coimbra, Almedina, 2010, cit., p. 83.

269 "I - O processo relativo à inibição e limitações ao exercício das responsabilidades parentais, regulado nos artigos 52.º a 59.º do RGPTC, tem natureza de processo de jurisdição voluntária, sendo-lhe também aplicável os artigos 986.º a 988.º do Código de Processo Civil. II - Os interesses nele em discussão são objecto de decisão a proferir segundo um juízo de oportunidade ou conveniência e não de estrita legalidade. III - A inibição do exercício das responsabilidades parentais em relação ao filho menor é uma medida de última ratio: só em situações em que os progenitores se comportem de forma grave e irreversível, colocando em risco, de forma grave, os interesses do menor podem ser inibidos do exercício das responsabilidades parentais relativamente a esse filho." Cf. Acórdão do Tribunal da Relação do Porto de 24/09/2020 (Relatora: Judite Pires), processo n.º 2747/06.9TQPRT-C.P1, disponível em <URL: http://www.dgsi.pt/>.

6. CONCLUSÃO

A incursão proposta por esta tese teve o propósito de apresentar o *sharenting* como fenomenologia dos dias hodiernos que atualiza as discussões relativas ao relacionamento entre pai e filhos, situando-as na era digital, tendo em vista a reflexão sobre os mecanismos de reação às consequências desvantajosas do fenómeno e a consequente proteção das crianças.

Como visto, não se pode dissociar a análise do *sharenting* da concepção pós-moderna que vê na criança e no adolescente pessoas munidas de dignidade, cujas especificidades exigem proteção da sociedade sem, no entanto, reduzi-las à incapacidade.

A ordem jurídica impõe, em verdade, a necessidade de respeito à personalidade dos filhos, sendo conferida, ao sujeito menor de idade, autonomia e uma *voz* condizente à sua maturidade (art. 1878.º, n.º 2, 2.ª parte, do Código Civil).

Nesta contextura, as responsabilidades parentais são reconfiguradas a "cuidado parental", ressaltando-se que o motor a orientar o exercício dos poderes-deveres de educação e proteção deve ser o primado do superior interesse da criança e do adolescente, pelo que a vontade dos progenitores não é prevalente quando a este seja oposta.

Essas premissas devem guiar o jurista quando a ele forem colocadas problemáticas associadas ao compartilhamento de informações pessoais das crianças pelos seus pais nas redes sociais.

Se é verdade que o direito não se pode alhear da realidade social, admitindo-se que as publicações em mídias sociais fazem parte da cultura digital do mundo em que hoje vivemos e são, genericamente, aceitas; também o é que, em hipótese de lesão ou ameaça de lesão à bem da personalidade, cumpre ao direito proporcionar meios de garantir o cessamento dessa ofensa, bem como a sua reparação.

Bem por isso, quando os pais extrapolem o exercício da sua liberdade de expressão e desrespeitem os deveres funcionais que lhe incumbem no exercício das responsabilidades parentais, ferindo o núcleo mais íntimo da personalidade dos filhos, deve-se entender cabível a adoção de providências ajustadas à conduta dos progenitores e ao grau do dano perpetrado.

Ao nosso ver, o instituto da responsabilidade civil, o direito ao "esquecimento digital" e a limitação do exercício às responsabilidades parentais representam soluções possíveis, em abstrato, de salvaguardarem os direitos à privacidade dos filhos, não podendo ser descartadas aprioristicamente. Aqui, a medida da proporcionalidade será de extrema valia para a construção da resposta adequada segundo as características que se apresentem no caso concreto.

7. BIBLIOGRAFIA

Albuquerque, Catarina, "Os Direitos da Criança em Portugal e no Mundo Globalizado: o princípio do interesse superior da criança" *in Direitos das Crianças*, Monteiro, A. Reis [Et Al], Coimbra, Coimbra Editora, 2004, pp. 39-63

Allen, Anita L., "Protecting One's Own Privacy in a Big Data Economy" *in Harvard Law Review Forum*, Vol. 130, 2016, pp. 71-78, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894545 (17.06.2022)

Almeida, João Paulo Simões De, "Os riscos da Internet para a privacidade: o caso português" *in Privacidade e comércio electrónico: Colóquio*, Lisboa, Comissão Nacional de Protecção de Dados, 2000, pp. 55-62

Ariès, Philippe, *História social da criança e da família*, 2ª ed, Rio de Janeiro, Guanabara Koogan S.A, 1978

Ascensão, José De Oliveira "A reserva da intimidade da vida privada e familiar" *in Revista da Faculdade de Direito da universidade de Lisboa*, Vol. XLIII, n.º 1, Coimbra Editora, 2002, pp. 9-25

Assis, Rui, "A reforma do direito dos menores: do modelo de proteção ao modelo educativo" *in Cuidar da Justiça de Crianças e Jovens: a função dos Juízes Sociais*, Sottomayor, Maria Clara [Et Al], Coimbra, Almedina, 2003, pp. 135-147

Barbosa, Mafalda Miranda, "Breves reflexões em torno do art. 127.º do Código Civil" *in Boletim da Faculdade de Direito – Universidade de Coimbra*, Vol. XC, Tomo II, Coimbra, 2014, pp. 685-717

Barbosa, Mafalda Miranda, "Família e responsabilidade civil: uma relação possível? Brevíssimo apontamento" *in Lex Familiae – Revista Portuguesa de Direito de Família*, Ano 10, n.º 20, Coimbra Editora, jul./dez. 2013, pp. 61-81

Barbosa, Mafalda Miranda, "Podem os pais publicar fotografias dos filhos menores nas redes sociais? Acórdão do Tribunal da Relação de Évora, 25 de junho de 2015" *in AB Instantia – Revista do Instituto do Conhecimento AB*, Ano III, n.º 5. Coimbra, Almedina, 2015, pp. 313-339

Barbosa, Mafalda Miranda, "Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil" *in AB Instantia – Revista do Instituto do Conhecimento AB*, Ano V, n.º 7, Coimbra, Almedina, 2017, pp. 13-47

Barroso, Luís Roberto, "Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa" *in Revista De Direito Administrativo*, Vol. 235, 2004, pp. 1-36, disponível em https://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/45123 (22.06.2022)

Bolieiro, Helena; Guerra, Paulo, *A criança e a família – uma questão de direito(s): visão prática dos principais institutos do direito da família e das crianças e jovens*, 2.ª ed., Coimbra, Coimbra Editora, 2014

Brosch, Anna, "When the Child is Born into the Internet: Sharenting as a Growing Trend among Parents on Facebook" *in The New Educational Review*, Vol. 43, n.º 1, 2016, pp. 225-235, disponível em https://tner.polsl.pl/issues/volume-432016 (20.09.2021)

C.S. Mott Children's Hospital, University Of Michigan System, *Parents on Social Media: Likes and Dislikes of Sharenting*, Vol. 23, n.º 2, 16/03/2015, disponível em https://mottpoll.org/sites/default/files/documents/031615_sharenting_0.pdf *(13.06.2022)*

Carvalho, Orlando De, *Teoria Geral do Direito Civil*, coordenação de Francisco Liberal Fernandes, Maria Raquel Guimarães, Maria Regina Redinha, 3ª ed., Coimbra, Coimbra Editora, 2012

Comissão De Direitos Da Família Europeu (CEFL), *Princípios de Direito de Família Europeu Relativo às Responsabilidades Parentais*, disponível em https://ceflonline.net/wp-content/uploads/Principles-PR-English.pdf (22.06.2022)

Conselho Da Europa, *Guidelines to respect, protect and fulfil the rights of the child in the digital environment: Recommendation CM/Rec(2018)7 of the Committee of Ministers, 2018*, disponível em https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html (15.06.2022)

Cordeiro, António Barreto Menezes, *Direito da proteção de dados: à luz do RGPD e da Lei n.º 58/2019*, 1ª ed., Coimbra, Almedina, 2020

Cordeiro, António Menezes Cordeiro, "Do abuso do direito: estado das questões e perspectivas" *in Revista da Ordem dos Advogados (ROA)*, Ano 65, Vol. II, Set. 2005, disponível em https://portal.oa.pt/publicacoes/revista-da-ordem-dos-advogados-roa/ano-2005/ano-65-vol-ii-set-2005/artigos-doutrinais/antonio-menezes-cordeiro-do-abuso-do-direito-estado-das-questoes-e-perspectivas-star/# (23.06.2022)

Cordeiro, António Menezes, *Tratado de direito civil, Vol. 4: Pessoas*; colab. A. Barreto Menezes Cordeiro, 5ª. ed., Coimbra, Almedina, 2019

Cruz, Rossana Martingo, "A divulgação da imagem do filho menor nas redes sociais e o superior interesse da criança" *in Direito e Informação na Sociedade em rede: Atas do IV Colóquio Luso-Brasileiro Direito e Informação*, 2016

DATAREPORTAL, Digital 2022 Global Digital Overview, 2022, disponível em https://datareportal.com/reports/digital-2022-global-overview-report (01.06.2022)

Dias, Cristina Manuela Araújo, "Responsabilidade civil e direitos familiares conjugais (pessoais e patrimoniais): possibilidade de indemnização ou fragilidade da garantia?" *in Scientia Ivridica – Revista de Direito Comparado Português e Brasileiro*, n.º 286/288, 2000

Dias, Cristina, "A criança como sujeito de direitos e o poder de correcção" *in Revista JULGAR*, n.º 4, 2008, pp. 87-101, disponível em http://julgar.pt/a-crianca-como-sujeito-de-direitos-e-o-poder-de-correccao/ (20.09.2021)

Duggan, Maeve [Et Al], *Parents and Social Media. Pew Research Center*, 2015, disponível em http://www.pewinternet.org/2015/07/16/parents-and-social-media/ (20.09.2021)

Eberlin, Fernando Büscher Von Teschenhausen, "Sharenting, liberdade de expressão e privacidade de crianças no ambiente digital: o papel dos provedores de aplicação no cenário jurídico brasileiro" *in Revista Brasileira de Políticas Públicas, Brasília*, Vol. 7, n.º 3, 2017, pp. 256-273, disponível em https://doi.org/10.5102/rbpp.v7i3.4821 (20.09.2021)

Erdos, David, "Intermediary publishers and European data protection: Delimiting the ambit of responsibility for third-party rights through a synthetic interpretation of the EU acquis" *in International Journal of Technology*, Vol. 26, n.º 3, 2018, pp. 189-225, disponível em https://academic.oup.com/ijlit/article/26/3/189/5033541 (30.06.2022)

Family Online Safety Institute, *Parents, Privacy and Technology Use,* 17/11/2015, disponível em https://fosi-assets.s3.amazonaws.com/media/documents/Full_Report--Web.pdf (13.06.2022)

Faria, Jorge Ribeiro De, *Direito das obrigações,* volume I, 2ª ed. atualizada e ampliada por Miguel Pestana de Vasconcelos e Rute Teixeira Pedro, Coimbra, Almedina, 2020

Farias, Cristiano Chaves De; Rosenvald, Nelson, *Curso de direito civil: parte geral e LINDB*, 19.ª ed., revista, ampliada e atualizada, Salvador: Ed. JusPodivm, 2021

Frada, Manuel A. Carneiro Da, "Nos 40 anos do Código Civil Português: tutela da personalidade e dano existencial" *in Themis, Revista de Direito*, Edição Especial, Lisboa, Faculdade de Direito da Universidade Nova de Lisboa, 2008, pp. 47-68

Godinho, Marteleto Adriano; Drumond, Marcela Maia De Andrade, "Autoridade parental: a autonomia dos filhos menores e a responsabilidade dos pais pela prática de cyberbullying" *in Autoridade Parental: dilemas e desafios contemporâneos*; coordenação de Ana Carolina Brochado, Luciana Dadalto, São Paulo: Editora Foco, 2019, pp. 169-185

Graux, Hans; Ausloos, Jef; Valcke, Peggy, "The right to be forgotten in the internet era" *in ICRI Research Paper*, n.º 11, 2012, disponível em https://ssrn.com/abstract=2174896. (25.06.2022)

Guichard, Raul, "Sobre a Incapacidade dos Menores no Direito Civil e a sua Justificação" *in Review of Business and Legal Sciences/Revista de Ciências Empresariais e Jurídicas*, n.º 6, pp. 103-148, 2005, disponível em https://doi.org/10.26537/rebules.v0i6.813 (20.09.2021)

Guimarães, Maria Raquel, "A Tutela da Pessoa e da sua Personalidade: algumas questões relativas aos direitos à imagem, à reserva da vida privada e à reserva da pessoa íntima ou direito ao caráter" *in A tutela geral e especial da personalidade humana – 2017*, 1ª. ed., Lisboa: Centro de Estudos Judiciários, 2018, pp. 25-47, disponível em https://cej.justica.gov.pt/LinkClick.aspx?fileticket=jEOZNTAE5L0%3d&portalid=30 (14.07.2022)

Hamming, Kate, "A Dangerous Inheritance: A Child's Digital Identity" *in SEATTLE U. L. REV.*, Vol. 43, n.º 3, 2020, pp. 1033-1063, disponível em https://digitalcommons.law.seattleu.edu/sulr/vol43/iss3/7/ (20.09.2021)

Harari, Yuval Noah, *Homo Deus: a brief history of tomorrow*, 1st edition, Vintage, 2017

Hinojo-Lucena, Francisco Javier [Et Al], "Sharenting: Internet addiction, self-control and online photos of underage children" *in Comunicar – Media Education Research Journal*, n.º 64, Vol. XXVIII, pp. 93-103, 2020, disponível em https://doi.org/10.3916/C64-2020-09 (20.09.2021)

Hörster, Heinrich Ewald, "A responsabilidade civil entre os cônjuges" *in E foram felizes para sempre...? Uma análise crítica do novo regime jurídico do divórcio. Actas do Congresso de 23, 24 e 25 de outubro de 2008*; coordenação de Maria Clara Sottomayor, Maria Teresa Féria de Almeida, Wolters Kluwer Portugal, Coimbra, Coimbra Editora, 2010, pp. 91-112

Lacerda, Bruno Torquato Zampier, *Bens digitais*, 2ª ed., São Paulo, Foco, 2021

Leal, Lívia Teixeira, "O Cuidado na era digital: as novas facetas da afetividade no mundo tecnológico e seus impactos jurídicos" *in Cuidado e Afetividade: projeto Brasil/Portugal, 2016-2017*, Pereira, Tânia Da Silva [Et Al], São Paulo, Atlas, 2017, pp. 267-290

Leandro, Armando, "Protecção dos direitos das crianças em Portugal" *in Direitos das Crianças*, Monteiro, A. Reis [Et Al], Coimbra, Coimbra Editora, 2004, pp. 101-119

Lopes, Inês Camarinha, "O consentimento como fundamento de licitude do tratamento de dados pessoais e o privacy paradox" *in O Sentir do Direito: Estudos em Homenagem ao Professor José Tavares de Sousa*; coordenação de André Lamas Leira, Fernando da Silva Pereira, Tiago Azevedo Ramalho, Lisboa, AAFDL – Associação Académica da Faculdade de Direito de Lisboa, 2022, pp. 197-217

Lopes, Inês Camarinha, *Os Dados Sensíveis dos Menores à Luz do RGPD*, Coimbra, GESTLEGAL, 1.ª. ed., 2021

Lopes, j. Seabra, "A proteção da privacidade e dos dados pessoais na sociedade de informação" *in Estudos dedicados ao Prof. Doutor Mário Júlio de Almeida Costa*, Silva, Germano Marques Da [ET. AL.], Lisboa, Universidade Católica Portuguesa, 2002, pp. 779-807

Marques, Paula Cristina Mariano, "Proteção ao direito de imagem da criança e do adolescente na internet" *in 3º Congresso Internacional de Direito e Contemporaneidade*, 2015, disponível em http://coral.ufsm.br/congressodireito/anais/2015/2-11.pdf (17.06.2022)

Martins, Rosa Cândido, "Poder paternal vs. autonomia da criança e do adolescente" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 1, n.º 1, Coimbra Editora, 2004, pp. 65-74

Martins, Rosa Cândido, "Responsabilidades parentais no século XXI: a tensão entre o direito de participação da criança e a função educativa dos pais" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 5, n.º 10, Coimbra Editora, 2008, pp. 25-40

Martins, Rosa, *Menoridade, (In)capacidade e Cuidado Parental*, Coimbra: Coimbra Editora, 2008

Melo, Helena Gomes De [Et Al], *Poder paternal e responsabilidades parentais*, 2.ª ed., Lisboa, Quid Juris, 2010

Mendes, João De Castro, *direito da família*, edição revista por Miguel Teixeira de Sousa, Lisboa, AAFDL, 1997

Minkus, Tehila; Liu, Kelvin; Ross, Keith W., "Children Seen But Not Heard: When Parents Compromise Children's Online Privacy" *in WWW'15: 24th International World Wide Web Conference*, 2015, pp. 776–786, disponível em https://dl.acm.org/doi/pdf/10.1145/2736277.2741124 (13.06.2022)

Miranda, Jorge; Medeiros, Rui, *Constituição Portuguesa anotada. Tomo I: Introdução geral, preâmbulo, artigos 1º a 79º*; colab. Maria da Glória Garcia [et. al.], 2ª ed., Coimbra, Wolters Kluwer Portugal, 2010

Moreira, Sónia, "A autonomia do menor no exercício de seus direitos" *in Scientia Ivridica*, Tomo L, n.º 291, Braga, Universidade do Minho, 2001, pp. 157-194

Oliveira, Guilherme De, "A criança maltratada" *in Interacções – Revista do Instituto Superior de Serviço Social de Coimbra*, n.º 1, 1995, pp.55-58

Oliveira, Guilherme De, "O acesso dos menores aos cuidados de saúde" *in Revista de Legislação e Jurisprudência*, ano 132, n.º 3898, 1999, pp. 16-18

Oliveira, Guilherme De, "Protecção de menores/Protecção familiar" *in Temas de Direito da Família, 1*, Coimbra, Coimbra Editora, 1999

Oliveira, Guilherme De, "Responsabilidade civil dos pais perante os filhos" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 18, n.º 35, Coimbra Editora, 2021, pp. 5-15;

Oliveira, Guilherme De, "Responsabilidade civil por violação dos deveres conjugais" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 16, n.º 31-32, Coimbra Editora, 2019, pp. 17-43

Organização Das Nações Unidas, Comité Dos Direitos Da Criança (CRC), *Comentário Geral n.º 25 (2021) sobre os direitos das crianças em relação ao ambiente digital*, 2021, disponível em https://gddc.ministeriopublico.pt/sites/default/files/documentos/pdf/crc-cg25-pt.pdf (13.06.2022)

Pedro, Rute Teixeira, "A responsabilidade Civil como (derradeira) manifestação de juridicidade dos deveres conjugais? Anotação ao Acórdão do Supremo Tribunal de Justiça (2.ª Secção) de 12.5.2016, Proc. 2325/12.3TVLSB.L1.S1" *in Cadernos de Direito Privado*, n.º 61, janeiro/março de 2018, pp. 52-62.

Pedro, Rute Teixeira, "A visão personalista da família e a afirmação de direitos individuais no seio do grupo familiar: a emergência de um novo paradigma decorrente do processo de constitucionalização do direito da família" *in Pessoa, Direito e Direitos: Colóquio 2014/2015*, Braga, Universidade do Minho, 2016

Pedro, Rute Teixeira, "Da ressarcibilidade dos danos não patrimoniais no direito português: a emergência de uma nova expressão compensatória da pessoa – Reflexão por ocasião do quinquagésimo aniversário do Código Civil" *in Estudos Comemorativos dos 20 anos da FDUP*, Vol. II, Coimbra, Almedina, 2017, pp. 681-712

Pedro, Rute Teixeira, "Os danos não patrimoniais (ditos) indiretos: uma reflexão ratione personae sobre a sua ressarcibilidade" *in Responsabilidade Civil: cinquenta anos em Portugal, quinze anos no Brasil*; coordenação de Mafalda Miranda Barbosa, Francisco Muniz, Coimbra, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, 2017, pp. 239-269

Pereira Coelho, Francisco; Oliveira, Guilherme De, *Curso de Direito da Família*, Vol. I, 5.ª ed., Rui Moura Ramos (colaborador), Coimbra, Imprensa da Universidade de Coimbra, 2018

Pinheiro, Alexandre Sousa, *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional*, Lisboa, AAFDL, 2015

Pinheiro, Jorge Duarte, "As crianças, as responsabilidades parentais e as fantasias dos adultos" *in Estudos de homenagem ao Prof. Doutor Jorge Miranda*, Vol. VI, Sousa, Marcelo Rebelo De [Et. Al.], Coimbra, Coimbra Editora, 2012, pp. 529-541

Pinheiro, Jorge Duarte, O Direito da Família Contemporâneo, Coimbra: GESTLEGAL, 7ª ed., 2020

Pinto, Carlos Alberto Da Mota; Monteiro, António Pinto; Pinto, Paulo Mota, *Teoria geral do direito civil*, Coimbra, Coimbra Editora, 5.ª ed., 2020

Pinto, Paulo Mota, "A limitação voluntária do direito à reserva sobre a intimidade da vida privada" *in Estudos em Homenagem a Cunha Rodrigues*, Vol. 2: Estudos variados, direito comunitário, Dias, Jorge Figueiredo [Et Al], Coimbra, Coimbra Editora, 2001, pp. 527-558

Pinto, Paulo Mota, *Direitos de personalidade e direitos fundamentais: estudos*, Coimbra, GESTLEGAL, 1ª ed., 2018

Portugal, Instituto Nacional De Estatística, *Inquérito à utilização de tecnologias da informação e da comunicação pelas famílias*, 2021, disponível em https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=473557834&DESTAQUESmodo=2 (01.06.2022)

Roque, Helder, "Os conceitos jurídicos indeterminados em Direito de Família e a sua integração" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 2, n.º 4, Coimbra Editora, 2005, pp. 93-98

Rosa, Conrado Paulino Da, *IFamily: um novo conceito de família?*, São Paulo, Saraiva, 2012

S/A, *Edição Comemorativa da Lei de Protecção da Infância, 27 de Maio de 1911*; coord. Carlos Poiares, Lisboa, Instituto da Segurança Social, 2010, disponível em https://www.cnpdpcj.gov.pt/documents/10182/14804/di%C3%A7%C3%A3o+-Comemorativa+da+Lei+de+Prote%C3%A7%C3%A3o+da+Inf%C3%A2ncia/f4726737-b519-4d49-a7f3-59ab3eda4cae (01.06.2022)

Sarkadi, Anna [Et Al], "Children want parents to ask for permission before sharenting" *in Journal of Paediatrics and Child Health*, 56, pp. 981-983, 2020, disponível em https://doi.org/10.1111/jpc.14945 (20.09.2021)

Shmueli, Benjamin; Blecher-Prigat, Avelet, "Privacy for Children" *in Columbia Human Rights Law Review*, Vol. 42, n.º 3, 2011, pp. 759-795, disponível em https://heinonline.org/HOL/P?h=hein.journals/colhr42&i=765 (20.09.2021)

Sorensen, Shannon, "Protecting Children's Right to Privacy in the Digital Age: Parents as Trustees of Children's Rights" *in Children's Legal Rights Journal*, Vol. 36, n.º 3, 2020, pp. 156-176, disponível em https://lawecommons.luc.edu/clrj/vol36/iss3/2/ (20.09.2021)

Sottomayor, Maria Clara, "A autonomia do direito das crianças" *in Estudos em Homenagem a Rui Epifânio*; coordenação de Armando Leandro, Álvaro Laborinho Lúcio, Paulo Guerra, Coimbra, Almedina, 2010, pp. 79-88

Sottomayor, Maria Clara, "Interesse da criança e ética do cuidado" *in Publicações ELSA Coimbra*, 1 de junho de 2021, disponível em https://clarasottomayor.com/public/files/interessecrianca.pdf (24.06.2021)

Sottomayor, Maria Clara, "Liberdade de opção da criança ou poder do progenitor? – comentário ao Acórdão do Tribunal da Relação de Coimbra, de 31 de outubro de 2007" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 5, n.º 9, Coimbra Editora, jan./jun. 2008, pp. 53-64

Sottomayor, Maria Clara, "O poder paternal como cuidado parental e os direitos da criança" *in Cuidar da Justiça de Crianças e Jovens: a função dos Juízes Sociais*, SOTTOMAYOR, MARIA CLARA [ET AL], Coimbra, Almedina, 2003, pp. 9-63

Sousa, Rabindranath Capelo De, "As alterações legislativas familiares recentes e a sociedade portuguesa" *in Textos de direito da família para Francisco Pereira Coelho*, OLIVEIRA, GUILHERME DE [coord.], Coimbra, Imprensa da Universidade de Coimbra, 2016, pp. 523-551

Steinberg, Stacey B., "Sharenting: Children's Privacy in the Age of Social Media" *in Emory Law Journal*, Vol. 66, n.º 4, 2017, pp. 839-883, disponível em https://scholarlycommons.law.emory.edu/elj/vol66/iss4// (20.09.2021)

Teixeira, Ana Carolina Brochado; Multedo, Renata Vilela, "(over)Sharenting e o abuso da conduta dos pais no ambiente digital" *in Direitos das Famílias e Sucessões na Era Digital*, Matos, Ana Carla Harmatiuk [Et Al], Belo Horizonte, Instituto Brasileiro de Direito de Família – IBDFAM, 2021, pp. 313-340

Teixeira, Ana Carolina Brochado; Multedo, Renata Vilela, "A responsabilidade dos pais pela exposição excessiva dos filhos menores nas redes sociais: o fenômeno do sharenting" *in Responsabilidade Civil e Direito de Família: O Direito de Danos na Parentalidade e Conjugalidade*, Matos, Ana Carla Harmatiuk [Et Al], Indaiatuba, Editora Foco, 2021, pp. 3-19

Unicef, *THE STATE OF THE WORLD'S CHILDREN 2017: Children in a digital world*, disponível em https://www.unicef.org/media/48581/file/SOWC_2017_ENG.pdf (01.06.2022)

Van Bueren, Geraldine, *International Documents on Children*, Second edition, Kluwer Law International, 1998

Varela, João De Matos Antunes, *Das obrigações em geral, Vol. I*, 10.ª. ed., Coimbra, Almedina, 2000

Vasconcelos, Pedro Pais De, *Direito de Personalidade*, Coimbra, Almedina, 2006

Vasconcelos, Pedro Pais De; Vasconcelos, Pedro Leitão Pais De, *Teoria Geral de Direito Civil*, 9.ª. ed., Coimbra, Almedina, 2019

Xavier, Rita Lobo, "Responsabilidades parentais no séc. XXI" *in Lex Familiae – Revista Portuguesa de Direito da Família*, Ano 5, n.º 10, Coimbra Editora, 2008, pp. 17-23

Xavier, Rita Lobo, *Recentes alterações ao regime jurídico do divórcio e das responsabilidades parentais*, Coimbra, Almedina, 2010

PÁGINAS DA *INTERNET* CONSULTADAS

Battersby, Lucy, "Millions of social media photos found on child exploitation sharing sites" *in The Sydney Morning Gerald*, 2015, disponível em https://www.smh.com.au/national/millions-of-social-media-photos-found-on-child-exploitation-sharing-sites-20150929-gjxe55.html (11.06.2022)

Castells, Manuel, "O digital é o novo normal" *in Fronteiras do pensamento*, 2020, disponível em https://www.fronteiras.com/leia/exibir/o-digital-e-o-novo-normal (01/06/2022)

Cheung, Helier, "Publicar fotos dos filhos nas redes sociais é invasão de privacidade?", *in BBC NEWS*, 2019, disponível em https://www.bbc.com/portuguese/geral-47731061 (06/06/2022)

Collins Dictionary, *Sharenting*, disponível em https://www.collinsdictionary.com/submission/11762/Sharenting (01/06/2022)

Gajanan, Mahita, "YouTube Star DaddyOFive Loses Custody of 2 Children Shown in 'Prank' Videos", *in TIME*, 2017, disponível em https://time.com/4763981/daddyofive-mike-martin-heather-martin-youtube-prank-custody/ (25/06/2022)

Google, *Ver páginas da Web em cache nos resultados da Pesquisa Google*, disponível em https://support.google.com/websearch/answer/1687222?hl=pt (01/06/2022)

Levin, Sam, "Couple who screamed at their kids in YouTube 'prank' sentenced to probationg"", *in The Guardian*, 2017, disponível em https://www.theguardian.com/us-news/2017/sep/12/youtube-parents-children-heather-mike-martin (25/06/2022)

Meakin, Nione, "The pros and cons of 'sharenting"", *in The Guardian*, 2013, disponível em https://www.theguardian.com/lifeandstyle/2013/may/18/pros-cons-of-sharenting (10/06/2022)

O'neill, Jennifer, "The Disturbing Facebook Trend of Stolen Kids Photos", *in Yahoo Parenting*, 2015, disponível em https://www.yahoo.com/news/mom-my-son-was-digitally-kidnapped-what-112545291567.html (10/06/2022)

S/A, "DaddyOFive parents lose custody 'over YouTube pranks"", *in BBC NEWS*, 2017, disponível em https://www.bbc.com/news/technology-39783670 (25/06/2022)

Urban Dictionary, *Sharenting*, disponível em https://www.urbandictionary.com/define.php?term=Sharenting (01/06/2022)

JURISPRUDÊNCIA CONSULTADA

Brasil, Tribunal de Justiça de São Paulo, Ap. Civ. n.º 1015089-03.2019.8.26.0577, 6ª Câmara de Direito Privado, Rel. Des. Vito Guglielmi, julgado em 13/07/2020

Portugal, Acórdão do N.º 181/97 do Tribunal Constitucional de 05/03/1997 (Relator: Luís Nunes de Almeida), disponível em http://www.tribunalconstitucional.pt/tc/acordaos/19970181.html

Portugal, Acórdão do Supremo Tribunal de Justiça de 27/01/2022 (Relator: Tomé Gomes), processo n.º 19384/16.2T8LSB-A.L1.S1, disponível em http://www.dgsi.pt/

Portugal, Acórdão do Supremo Tribunal de Justiça de 16/11/2021 (Relatora: Maria Clara Sottomayor), processo n.º 21827/17.9T8SNT-A.L1.L1.S1, disponível em http://www.dgsi.pt

Portugal, Acórdão do Tribunal da Relação de Évora de 25/06/2015 (Relator: Bernardo Domingos), processo n.º 789/13.7TMSTB-B.E1, disponível em http://www.dgsi.pt/

Portugal, Acórdão do Tribunal da Relação de Lisboa de 07/10/2021 (Relator: Jorge Leal), processo n.º 58/20.6T8SCG.L1-2, disponível em http://www.dgsi.pt/

Portugal, Acórdão do Tribunal da Relação de Lisboa de 02/05/2017 (Relator: Pedro Brighton), processo n.º 897/12.1T2AMD-F.L1-1, disponível em http://www.dgsi.pt/

Portugal, Acórdão do Tribunal da Relação do Porto de 10/02/2022 (Relatora: Aristides Rodrigues de Almeida), processo n.º 3323/18.9T8VFR-A.P1, disponível em http://www.dgsi.pt/

Portugal, Acórdão do Tribunal da Relação do Porto de 12/10/2021 (Relatora: Anabela Dias da Silva), processo n.º 8369/17.1T8VNG.P1, disponível em http://www.dgsi.pt/

Portugal, Acórdão do Tribunal da Relação do Porto de 24/09/2020 (Relatora: Judite Pires), processo n.º 2747/06.9TQPRT-C.P1, disponível em http://www.dgsi.pt/

Portugal, Acórdão do Tribunal da Relação do Porto de 27/01/2020 (Relator: José Eusébio Almeida), processo n.º 803/13.6T2OBR-D.P1, disponível em http://www.dgsi.pt/

União Europeia, Tribunal de Justiça da União Europeia, Grande Secção, Acórdão de 13/05/2014, processo nº C-131/12, Google Spain SL, Google Inc. contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González, disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9959369

INTERNET DAS COISAS E PROTEÇÃO DE MENORES ENQUANTO CONSUMIDORES

Joseanne Correia Martins de Barros Couto

Resumo: O hodierno e crescente desenvolvimento tecnológico transforma a sociedade mundial e atua significativamente em todos os setores económicos e socias. Em particular, as tecnologias da Internet das Coisas trouxeram novas oportunidades para os seus utilizadores, assim como desafios relacionados com a proteção dos seus direitos. O presente trabalho visa discutir o uso e consumo das tecnologias pertencentes à Internet das Coisas pelos "consumidores-crianças". Denota-se que as crianças contemporâneas têm consumido cada vez mais produtos inteligentes, embora nem sempre estejam aptas ou preparadas para a utilização dos mesmos. É um fenómeno que merece atenção, porque o menor é um ser humano vulnerável que carece de uma proteção jurídica forte para garantia e respeito dos seus direitos face ao mundo digital.

O propósito desta dissertação de mestrado é analisar os traços gerais dos objetos inteligentes e demostrar os potenciais efeitos jurídicos que os mesmo podem provocar na esfera jurídica dos menores, em especial, os impactos negativos oriundos de falhas de segurança advindas de produtos inteligentes defeituosos disponíveis no tráfego jurídico. Ver-se-á neste trabalho, a posição jurídica do menor num mundo cada vez mais conectado, em particular, no âmbito do uso e consumo de tecnologias inteligentes, e analisar-se-ão os novos desafios, em matéria de segurança e responsabilidade, que estes aparelhos têm colocados ao Direito.

Palavras-chaves: Internet das Coisas, menores, produtos defeituosos, responsabilidade do produtor, segurança do produto.

Abstract: The growing technological development transforms the world society and acts significantly in all economic and social sectors, particularly technologies associated with the Internet of Things that have brought new opportunities for its users, as well as challenges related to the protection of their rights. The present work aims to discuss the use and consumption of those technologies by child consumers. It is noted that contemporary children have been using more smart devices, although they are not always able or prepared to use them. It is a phenomenon that deserves attention because minors are vulnerable human beings who lack strong legal protection to guarantee and respect their rights in the digital world.

This master's thesis purpose is to analyze the main features of smart objects and demonstrate the potential legal effects they can cause in the legal sphere of minors, especially the negative impacts arising from security failures originating from defective devices available in legal matters. In this paper, we will see the legal position of the minor in an increasingly connected world, particularly in the context of the use and consumption of smart technologies, and analyze the new challenges in terms of safety and responsibility that these devices have posed to the Law.

Keywords: Internet of Things, minors, defective devices, producer responsibility, product safety

1. INTRODUÇÃO

Nos últimos vinte anos, as novas tecnologias da informação e da comunicação desenvolveram-se e têm transformado profundamente todas as estruturas económicas e sociais da humanidade. O acesso e o uso habitual da *Internet* no dia a dia, o incremento da oferta de produtos e serviços digitais, a propagação e o aperfeiçoamento das tecnologias já existentes, são alguns acontecimentos que têm propulsionado mudanças significativas no funcionamento das nossas sociedades. Hoje em dia, há setores inteiros da economia mundial e da vida privada com base na automatização e na comunicação, realizadas exclusivamente com e através das máquinas. Encontramos esta revolução na agricultura, nos transportes, na área da saúde, na produção industrial, em aparelhos domésticos e muitos outros.

Indubitavelmente, essas mudanças têm-se refletido na vida dos cidadãos, nomeadamente na vida dos mais novos, que são frequentemente imersos num ecossistema conectado, onde pessoas e objetos estão em constante ligação. O universo das novas tecnologias é uma realidade bem presente e a tendência é que ele se acentue ainda mais nas próximas décadas.

Perante a corrente revolução tecnológica, constatamos que os consumidores têm demostrado particular interesse por produtos e serviços pertencentes à *Internet of Things,* (na tradução portuguesa *Internet das Coisas*). Na prática, estes bens de consumo são itens utilizados no dia a dia, como por exemplo, uma televisão ou um relógio de pulso; todavia possuem uma particularidade distintiva: eles têm a capacidade de interagir com o seu utilizador através da sua conexão à Internet ou a outros dispositivos, oferecendo uma experiência personalizada e única ao seu consumidor. Como resultado, as IdC (acrónimo para Internet das Coisas) têm atraído e têm sido produto de eleição perante os mais novos, que estão diariamente expostos ao uso e ao consumo de produtos e serviços conectados. Como resultado, as crianças tornaram-se um dos principais alvos da indústria das tecnologias pertencentes a IdC. Hoje em dia, há produtos e serviços inteligentes concebidos exclusivamente para satisfazer as suas necessidades e interesses. São inúmeras as oportunidades que estes dispositivos oferecem. Todavia, as interligações do ambiente conectado também dão espaço a violações de direitos e ameaçam interesses jurídicos protegidos pela ordem jurídica interna e internacional, que, por sua vez, produzem vários ilícitos, como por exemplo, pornografia infantil, aliciamento de menores, tratamento não autorizado de dados pessoais do menor, intrusão indevida na sua vida privada e familiar, etc. Além destes, reparamos que a segurança da criança é comprometida devido a violações de direitos do consumidor relacionados com as falhas de seguranças que os produtos inteligentes podem apresentar. Diante deste problema, o assunto torna-se ainda mais delicado, pois as crianças, devido à sua especial condição de vulnerabilidade relacionada com as suas capa-

cidades psíquica e física não estarem completamente desenvolvidas, merecem uma proteção e um tratamento diferenciado.

Face a esta nova realidade, a presente dissertação de mestrado pretende discutir os impactos nefastos que dispositivos inteligentes provocam na vida dos menores, em especial, os danos oriundos de falhas de segurança no produto inteligente.

Para tal, trataremos da posição da criança enquanto titular de direitos e garantias, num mundo cada vez mais conectado. Em primeiro lugar, falaremos dos direitos do infante no ordenamento jurídico português, de seguida, debruçar-nos-emos na descoberta das tecnologias pertencentes ao universo da Internet das Coisas. Nesta parte do trabalho, descreveremos aspetos técnicos dos dispositivos inteligentes e enunciaremos alguns aparelhos inteligentes com que as crianças portuguesas têm mais contacto. No terceiro capítulo, estudaremos a categoria jurídica de "consumidor-criança", antes de falarmos da proteção dos seus direitos face a dispositivos inteligentes defeituosos. Veremos, neste último capítulo, os novos desafios que os produtos inteligentes têm trazido ao Direito, em especial, em matéria de segurança do produto e da responsabilidade do produtor.

2. OS DIREITOS DA CRIANÇA NO ORDENAMENTO JURÍDICO PORTUGUÊS

O século XXI é marcado por uma sociedade dita "da informação", na qual a globalização apagou fronteiras virtuais e fez surgir um novo espaço totalmente volátil, difícil de acompanhar pela sua constante transformação. Esta realidade é propulsionada pelas novas tecnologias, entre as quais, destacamos a Internet das Coisas.

Indubitavelmente, o novo cenário trouxe mudanças para a vida das crianças. Por um lado, ele trouxe-lhes oportunidades, como brincar e aprender, mas também trouxe preocupantes riscos para as suas esferas jurídicas, que "multiplicam-se todos os dias e, sobretudo, diversificam-se, ao mesmo ritmo que se desdobram os meios tecnológicos postos à disposição dos consumidores"[1]. Deste modo, o ambiente digital apresenta-se como uma área nebulosa para o Direito, pois nem sempre sabemos quais os reais impactos que os dispositivos inteligentes poderão causar na vida dos menores, que pelas suas incapacidades psíquica, intelectual, social e física, merecem um tratamento diferenciado, razões pelas quais o Direito atribui uma proteção especializada, e um estatuto civil particular, chamado de menoridade.

[1] Maria Regina Redinha e Maria Raquel Guimarães - "O uso do correio eletrónico no local de trabalho: algumas reflexões". In - *Estudos em homenagem ao Professor Doutor Jorge Ribeiro de Faria* [Em linha]. 2003. [Consult. 2021-08-24]. Disponível na Internet: <URL: https://repositorio-aberto.up.pt/handle/10216/24325>.

Face à temática da proteção e promoção dos direitos da criança, Portugal reconhece o menor como sujeito autónomo titular de Direitos Humanos. A sua proteção e o seu reconhecimento no nosso ordenamento jurídico, são fruto de uma evolução acentuada, que perdura até aos dias de hoje, devido aos desafios diários oriundos da sociedade volátil na qual estamos inseridos.

Em Portugal, a criança é reconhecida e vista como um ente em contínuo desenvolvimento. Ela é protegida pelo viés de diplomas de fonte internacional, comunitária e nacional, que reconhecem a importância da qualidade da infância e defendem que ela é um requisito insubstituível para o desenvolvimento do ser humano, a todos os níveis, nomeadamente ético, cívico, cultural, científico, social, ambiental e económico[2].

O sistema português de proteção e promoção dos Direitos das Crianças está atento e disposto a aplicar aperfeiçoamentos e atualizações que sejam necessárias para garantir e promover os direitos das crianças. Ademais, ele considera os dados sobre a evolução dos complexos contextos[3], nomeadamente, diante dos novos desafios provenientes das tecnologias da IdC, para assegurar que a criança seja protegida em qualquer situação.

Posto isto, o presente capítulo servirá de análise de alguns direitos e garantias que o Sistema Jurídico consagra aos menores em Portugal, que julgamos ser imprescindíveis para o tema. Para esse fim, optamos, dentro do vasto leque normativo em vigor, por percorrer alguns preceitos da Constituição da República Portuguesa (CRP), que julgamos serem relevantes para o desenvolvimento da nossa dissertação. De seguida, abordaremos um recente diploma, que, pelo seu conteúdo, se apresenta significativo para a promoção e proteção dos direitos dos menores na era digital: "Carta Portuguesa de Direito Humanos na Era Digital". Por último, estudaremos a menoridade estatuída no Código Civil, de modo a extrairmos uma noção operacional de "menor" e discutirmos o seu real significado face às novas tecnologias.

---

[2] armando Leandro - "Promoção e Proteção dos Direitos da Criança". *Boletim da Ordem dos Advogados*. Ordem dos Advogados. [Em linha]. (2019) [Consult. 2021-07-29]. Disponível na Internet: <URL: https://boletim.oa.pt>. p. 24-25. O juiz defende que o atual "sistema que dispomos de promoção e proteção é um amplo Sistema de promoção e proteção, que engloba várias outros subsistemas", entre eles o subsistema de promoção e proteção, o tutelar educativo, o tutelar cível etc. Dito isto, devemos continuar a promover e proteger os direitos dos menores em todos os âmbitos já consagrados, e quando for caso, estender a proteção a outros âmbitos para, assim, assegurar sempre os direitos dos menores, assim como as suas liberdade e garantias.

[3] armando Leandro - "Promoção e Proteção dos Direitos da Criança". *Boletim da Ordem dos Advogados*. cit. p. 29. O autor conclui no ponto 9. que ".... temos um Sistema que, pela natureza e harmonia dos seus fundamentos e características, é em si mesmo um Sistema intrinsecamente integrativo, por isso validamente "amigo" e fortemente protetor da execução sistemática e integrada...".

2.1. OS DIREITOS DA CRIANÇA NA CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA

A Constituição da República Portuguesa (CRP) ocupa a posição de lei suprema na ordem jurídica portuguesa e, como tal, ela apresenta-se como referência em matéria de promoção e proteção dos direitos da criança. Ela dispõe de normas que visam proteger os bens e os interesses dos menores, na forma de direitos fundamentais ou na forma de verdadeiros deveres impostos ao Estado e a sociedade.

Em primeiro lugar, destacamos o art. 8.º da CRP que consagra o sistema de receção automática de normas de direito internacional e comunitário dos Tratados que foram devidamente ratificados ou aprovados, e assim, Portugal acolhe para o seu ordenamento jurídico, disposições de fonte externa.

Em especial, destacamos dois diplomas importantíssimos em matéria de proteção e promoção de direitos das crianças: a Convenção das Nações Unidas dos Direitos da Criança[4] e a Convenção Europeia sobre os Direitos da Criança[5]. Em segundo plano, frisamos o facto de a lei suprema não estabelecer um conceito para o termo "criança". Por conseguinte, e por força do art. 8.º, adotamos a noção estatuída pela Convenção dos Direitos da Criança, que define o seu art. 1.º, criança como "todo o ser humano com menos de 18 anos, salvo se, nos termos da lei que lhe for aplicável, atingir a maioridade mais cedo".

Ademais, invocamos o art. 1.º da CRP que consagra um princípio de teor imprescindível para promoção e proteção dos direitos da criança: o princípio da dignidade humana. Segundo o professor Gomes Canotilho "trata-se de um princípio antrópico que recolhe a ideia [...] da *dignitas-hominis*[6]*",* isto é, reconhecemos a criança como "alguém que pode assumir a condição de cidadão, ou seja, um membro normal e plenamente cooperante ao longo da sua vida[7]".

Nesta lógica, conjugando o art. 8.º com o princípio da dignidade humana, concluímos que os menores são indivíduos titulares de direitos, liberdades e garantias consagrados em convenções internacionais, na lei suprema, na legislação ordinária, e em todos dos documentos legislativos que lhe dizem respeito, direta ou indiretamente.

---

[4] A Convenção das Nações Unidas dos Direitos da Criança, entrou, entre nós, em vigor pela Resolução da Assembleia da República n.º 20/90, de 12 de setembro, que aprova, para ratificação, a Convenção sobre os Direitos da criança, assinada em Nova Iorque a 26 de janeiro de 1990. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1894&tabela=leis.

[5] A Resolução da Assembleia da República n.º 7/2014, aprova a Convenção Europeia sobre o Exercício dos Direitos das Crianças, adotada em Estrasburgo, em 25 de janeiro de 1996. Disponível em https://dre.pt/application/file/a/571090.

[6] josé Joaquim Gomes Canotilho - *Direito constitucional e teoria da constituição.* 7ª ed. Coimbra: Almedina, 2018. ISBN: 978-972-40-2106-5. p. 225.

[7] josé Joaquim Gomes Canotilho - *Direito constitucional e teoria da constituição*, cit., p. 225.

Além disso, ainda na combinação das normas mencionadas, a criança tem o direito de participar em todas as decisões que lhe digam respeito e devem ser sempre ouvidas, sobretudo nas tomadas de decisões políticas que interfiram nas suas vidas. Afinal, ela é considerada, como explicou Gomes Canotilho, "um ser cooperante ao longo da sua vida"[8].

Agora que já percebemos que a criança é titular de direitos, liberdades e garantias, cabe-nos averiguar quem são aqueles que assumem o papel de protetor e provedor dos seus direitos, tanto no mundo "online", como no mundo "offline". Nesse sentido, avançamos no diploma constitucional e vemos que o art. 69.º, n.º 1 da CRP determina que o dever de proteção e promoção da infância cabe essencialmente ao Estado e à sociedade. No fundo, esta disposição impõe deveres — ao Estado, às entidades públicas e à sociedade em geral — de eliminarem, tanto quanto possível, todos os fatores geradores de perigo aos direitos dos infantes. A norma estabelece que os referidos agentes devem criar e aplicar legislação necessária para promoção e proteção dos direitos infantis, e praticar ações administrativas adequadas com vista a garantir a concretização desses direitos.

Ora, face à rápida evolução do mundo digital e diante da factualidade dos dispositivos inteligentes serem partes integrantes do quotidiano dos menores, há uma necessidade alarmante de assegurar os direitos das crianças independentemente do ambiente em que eles são chamados a atuar[9]. Neste sentido, é necessário que o Estado e a sociedade intensifiquem os seus esforços para proteger os mais novos do ecossistema digital, cobrindo e dando respostas às oportunidades e desafios colocados.

Além do Estado e da sociedade, recai sobre os pais um papel importante na proteção dos menores (art. 36.º, n.º 5). Os progenitores têm o dever de assegurar o desenvolvimento completo da criança, cabendo-lhes os papéis imprescindíveis de educar, cuidar e garantir o seu desenvolvimento integral[10]. Desta maneira, os infantes serão capazes de fazer face às novas tecnologias e ao ambiente conectado da Internet das Coisas[11].

---

[8] josé Joaquim Gomes Canotilho - *Direito constitucional e teoria da constituição*, cit., p. 225.

[9] Sara Pereira - "Os direitos da criança no mundo digital". *Forum de proteção de dados*. Lisboa: Comissão Nacional de Protecção de Dados. [Em linha]. Vol: [6 vol.] (2019) p. 8-17. Disponível na ISSN: 2183-5977. p. 9-16.

[10] josé Joaquim Gomes Canotilho e Vital Moreira - *Constituição da República Portuguesa anotada*. 4ª rev. ed. Coimbra: Coimbra Editora, 2007. ISBN: 972-32-1462-8. p. 869.

[11] Ao nosso ver, a dimensão desta norma é bastante densa e o seu cumprimento apresenta algumas dificuldades. Com sucintas palavras, ela traduz-se na responsabilidade dos representantes legais assegurar e garantir que seus filhos sejam aptos, ou pelo menos capazes de fazer face aos desafios criados pelas novas tecnologias e pelo ambiente conectado, quando os progenitores desconhecem os riscos advindos do mundo digital, e/ou não tem os conhecimentos, nem habilidades necessárias para assegurar a educação e segurança dos seus filhos.

Proteger as crianças é, portanto, em qualquer circunstância e em qualquer espaço, seja ele virtual, seja ele físico, um labor coletivo. Todos temos um papel a desempenhar para alcançar um ambiente digital menos poluído de ciberameaças, e consequentemente, um espaço onde há respeito pelas crianças e pelos seus direitos[12].

Concluímos assim, que a ordem constitucional portuguesa tenta proteger e promover os direitos das crianças face a todas as realidades, inclusive, diante das tecnologias da IdC. Ela estatui o menor como titular de direitos, liberdades e garantias provenientes de várias fontes jurídicas e, ainda, mobiliza todos os agentes da sociedade para assegurar a infância de qualquer cidadão. No entanto, apesar da sua eficácia e teor imprescindível, é preciso estarmos sempre atentos às transformações sociais, nomeadamente, àquelas oriundas do ambiente conectado. Pela sua célere expansão e novidades, as tecnologias da IdC colocam, diariamente, novos desafios à ordem jurídica. Por isso, o labor para uma proteção constitucional é constante, e não só, devemos medir sempre os nossos melhores esforços para garantir um ecossistema seguro para as nossas crianças. Neste sentido, o sistema jurídico português, com vista a consagrar e tutelar direitos, liberdades e garantias dos utilizadores da internet — inclusive os infantes— no ambiente digital, emanou recentemente a Carta Portuguesa de Direitos Humanos na Era Digital. Assim sendo, dedicaremos o próximo ponto da nossa dissertação ao estudo deste instrumento, que julgamos ser rico para o tema.

2.2. A CARTA PORTUGUESA DE DIREITOS HUMANOS NA ERA DIGITAL

A República Portuguesa está inserida no processo mundial das transformações tecnológicas provenientes da Internet. Além disso, ela está atenta à envolvência das suas crianças e dos seus jovens com as tecnologias da IdC, e tem consciência que eles nem sempre estão preparados para fazer face aos desafios e aos riscos colocados pelo ambiente digital. Reconhecendo a necessidade de assegurar os seus direitos, liberdades e garantias na era digital atual, foi emanada a Lei n.º 27/2021, de 17 de maio, que aprova a Carta Portuguesa de Direitos Humanos na Era Digital.

Antes de mais, esta Carta garante que as normas — pré-existentes e vigentes — que consagram e tutelam direitos, liberdades e garantias na ordem jurídica portuguesa são plenamente aplicáveis no ciberespaço (art. 2.º, n.º 2). Verdadeiramente, este diploma veio reforçar o teor e âmbito de aplicação dos mesmos, assim como consagrar novos direitos, como é o caso do direito ao testamento digital (art. 18.º).

Sublinhamos, no entanto, que iremos, ao longo desta dissertação, invocar e detalhar com mais afinco alguns dos direitos consagrados neste instru-

12 Sara Pereira - "Os direitos da criança no mundo digital". *Forum de proteção de dados*. cit. p. 9-16.

mento normativo, como o direito à privacidade em ambiente digital (art. 8.º), o direito ao desenvolvimento de competências digitais (art. 9.º), o direito ao esquecimento (art. 13.º), o direito à cibersegurança (art. 15.º), e o direito à proteção contra a geolocalização abusiva (art. 17.º). Porém, e por agora, dedicar-nos-emos, exclusivamente, ao art. 20.º que é aquele que consagra os direitos das crianças na era digital.

Aferimos que o conteúdo normativo do art. 20.º é, no fundo, o reforço de alguns direitos já consagrados na Convenção dos Direitos da Criança. Atentos à leitura do n.º 1, do art. 20.º: "As crianças têm o direito à proteção especial e aos cuidados necessários ao seu bem-estar e segurança no ciberespaço", revemos o conteúdo normativo do art. 6.º da Convenção dos Direitos da Criança (CDC), que reconhece o direito à vida, à sobrevivência e ao desenvolvimento da criança. Na prática, a consagração deste preceito impõe aos Estados signatários a obrigação de prestarem atenção às várias facetas do desenvolvimento do menor. Neste sentido, a República Portuguesa deve ter sempre atenção aos impactos que os aparelhos inteligentes podem causar na vida do menor, de maneira a não perturbar o seu pleno desenvolvimento. Nesta lógica, Portugal deve criar e proporcionar todos os meios e todas as medidas necessárias e adequadas para preparar todas as crianças para uma vida individual sana, numa sociedade digital [13].

Simultaneamente, apercebemo-nos ainda no art. 20.º, n.º 1, da Carta Portuguesa de Direitos Humanos na Era Digital*,* a *ratio* do princípio do interesse superior da criança estatuído no art. 3.º da CDC. Tal princípio assegura que todas as decisões que digam respeito, direta ou indiretamente, às crianças devem ser tomadas com vista a satisfazer o seu interesse superior. Ou seja, Portugal deve garantir que todas as decisões tomadas, relativamente à proteção, aos cuidados necessários, ao seu bem-estar e à segurança do menor no ciberespaço, sejam fundamentadas em prol do seu melhor interesse.

Complementarmente, o art. 20.º, n.º 2, determina que "As crianças podem exprimir livremente a sua opinião e têm a liberdade de receber e transmitir informações ou ideias, em função da sua idade e maturidade". Neste número, vemos nitidamente, o conteúdo normativo do art. 12.º da CDC que elenca o "respeito pela opinião da criança". Em breves palavras, respeitar a opinião

---

[13] patrícia Brander, Laure De Witte [et.al.] - *Compass* [Em linha]. 1ª ed. Guide - Artes Gráficas, Lda., 2016. [Consult. 2021-04-19]. Disponível na Internet: <URL: https://www.dge.mec.pt/compass-manual-de-educacao-para-os-direitos-humanos-com-jovens>. ISBN 978-989-99443-1-2. p. 436. "A CDC foi um passo gigante para começar o processo da formalização das obrigações governamentais e de alguma forma de cobrança de responsabilidade. Contudo, foi apenas o início de um processo. Em todos os países do mundo, os Direitos da Criança têm ainda um longo caminho a percorrer antes de alcançarem os padrões definidos na Convenção.".

da criança é um direito de aplicação obrigatória[14], que impõe aos Estados signatários o dever de sempre ouvir a opinião dos menores de modo a assegurar o seu direito fundamental de liberdade de expressão e garantir que as suas opiniões sejam tidas em consideração no seu contexto familiar, escolar, nos locais de cuidado institucional, entre outros[15], e isto aplica-se igualmente no contexto digital. No fundo, dar voz às crianças é dar-lhes visibilidade, é inclinar-se para ouvir e perceber as suas dúvidas, medos e vontades e assim legislar ao encontro das suas reais necessidades.

A Carta Portuguesa de Direitos Humanos na Era Digital mostra-se como um instrumento normativo que veio reforçar direitos essenciais e intrínsecos à proteção e promoção dos direitos da criança, mas, mais especificamente, no âmbito digital.

2.3. O CONCEITO DA MENORIDADE NO DIREITO CIVIL PORTUGUÊS

Aquando do seu nascimento, completo e com vida, a criança adquire personalidade jurídica (art. 66.º do Código Civil). Nas palavras de Orlando de Carvalho, o direito geral de personalidade enquanto um "direito à pessoa-ser e à pessoa-devir[16]", está assente no reconhecimento da criança como pessoa humana. Ele permite que o menor seja tutelado em todas as manifestações possíveis da sua personalidade, quer as previsíveis, quer as imprevisíveis. No fundo, é um direito vertido numa cláusula geral — no art. 70.º do Código Civil — mas que admite simultaneamente que haja direitos especiais de personalidade, particularizando a tutela geral consagrada[17].

A ordem jurídica portuguesa elenca, nos arts. 122.º a 133.º do Código Civil (CC), disposições normativas vocacionadas para a estatuição da condição jus civilística da menoridade. Apesar de o legislador português não formular uma concreta definição do conceito de menoridade, ele acolheu, em alternativa, o sistema de fixação normativa da maioridade[18]. Fundamentalmente, este sis-

---

[14] isabel Cunha Gil - Sinfonia do Supremo interesse da criança. *Boletim da Ordem dos Advogados*. Ordem dos Advogados. [Em linha]. (2019) [Consult. 2021-07-29]. Disponível na Internet: <URL: https://boletim.oa.pt>. p. 9. A autora, referindo-se a comemorações dos 20 anos da CDC escreveu que "Ficou claro, no discurso de todas as crianças que participara nessa sessão, que querem participar ativamente em todas as decisões que lhe dizem respeito, que querem ser ouvidas sobre as suas visões relativas as questões sociais, questões ambientais ... A Declaração dos Direito da Criança trouxe a criança para dentro do princípio da dignidade, passando a ser encarada como qualquer outro ser humano."

[15] patrícia Brander, Laure De Witte [et.al.] - *Compass* cit., p. 436. "quando os Estados reportam ao Comité dos Direitos da Criança, espera-se que evoquem as oportunidades das crianças para expressarem as suas opiniões no contexto da vida familiar, escolar, locais de cuidado institucional ou outros, bem como nos processos de requisição de asilo.".

[16] Orlando De Carvalho - *Teoria geral do direito civil* 3ª ed. Coimbra: Coimbra Editora 2012. ISBN: 978-972-32-2017-9. p. 90.

[17] Nesse sentido, *vide* Maria Regina Redinha [et.al.], cit., p. 652.

[18] João de Castro Mendes - *Direito civil: teoria geral* 2ª ed. ed. 1978. p. 128. João Mendes explica que Portugal optou por acolher o sistema da maioridade civil, tal como "... a

tema determina que "aquele que perfizer dezoito anos de idade adquire plena capacidade de exercício de direitos, ficando habilitado a reger a sua pessoa e a dispor dos seus bens". Com outras palavras, a lei civil estabelece, no seu art. 130.º, que uma pessoa não alcança a maioridade enquanto não tiver completado dezoitos anos. Por sua vez, o art. 1º da CDC considera criança, como vimos, quem não tiver completado 18 anos[19]. Posto isto, concluímos com a conjugação dos dois preceitos, que crianças são todos aqueles com menos de dezoito anos.

Frisamos, no entanto, que a menoridade civil é mais do que uma fixação normativa, ela representa o primeiro estado de vida de qualquer ser humano. Como referiu Rosa Martins, a maioridade dá-se no final de um processo de amadurecimento gradativo ao qual o ser humano se submete desde o seu nascimento[20]. Uma criança é um ser em desenvolvimento, que exige um "tratamento autónomo do adulto, quer para a sua proteção quer para sua responsabilização"[21]. Nesses termos, a menoridade é o primeiro período da vida de um indivíduo que é limitado, segundo o art. 123.º do CC, por uma incapacidade relacionada com o seu desenvolvimento incompleto. Desta forma, os menores, até completarem dezoito anos de idade, carecem de capacidade para o exercício de direitos.

Contudo, o mesmo preceito que determina a incapacidade dos menores também faz uma ressalva "salvo disposição em contrário", que atenua a rigidez do regime e possibilita várias exceções a incapacidade geral, que será atribuída em função do gradual desenvolvimento do menor. Entre elas encontramos àquelas que estão consagradas no art. 127.º do CC que teremos a oportunidade de abordar, no ponto 3 da presente dissertação.

Ademais, segundo o art. 124.º do CC, a incapacidade de exercício do menor é suprível pelos meios postos à disposição pelo instituto da representação, que são em primeira linha, as responsabilidades parentais (n.º 1 do art. 1878.º do CC), e subsidiariamente, a tutela (art. 1921.º do CC); eventualmente poderá

grande maioria das ordens jurídicas segue um sistema de fixação normativa da maioridade."

[19] Menciona o artigo 1.º da Convenção sobre os Direitos da Criança: "Nos termos da presente Convenção, criança é todo o ser humano menor de 18 anos, salvo, se, nos termos da lei que lhe for aplicável, atingir a maioridade mais cedo." (Pode ser consultado em: https://www.unicef.pt/media/2766/unicef_convenc-a-o_dos_direitos_da_crianca.pdf)

[20] rosa Martins - *Menoridade, (in)capacidade e cuidado paternal*. ed. Coimbra: Coimbra Editora, 2008. ISBN: 978-972-32-1591-5. p. 25-29. A autora acrescenta ainda que "Este sistema baseia-se num critério puramente casuístico de averiguação do momento em que cada sujeito atinge o grau de desenvolvimento das suas faculdades dísicas, intelectuais, morais e emocionais que garante maturidade e experiência características de uma situação de autonomia e independências.".

[21] armando Leandro - "Promoção e Proteção dos Direitos da Criança". *Boletim da Ordem dos Advogados*. cit. p. 26. Referindo-se ao sistema de promoção e proteção dos diretos das crianças, o juiz conselheiro Armando Leandro pronunciou: "A consideração da criança não como adulto mais novo, mas como um "outro", um ser diferente, em específico desenvolvimento, a exigir tratamento autónomo do adulto, quer na proteção, que na responsabilização...".

haver lugar à instituição, com os mesmos fins, do regime de administração de bens (art. 1922.º do CC)[22].

Em conclusão, consideramos criança todo o ser humano que não tenha completado 18 anos de idade. Este indivíduo é titular de direitos, liberdades e garantias, que devem ser sempre asseguradas, independentemente do meio em que estiver inserido. Os mais novos sofrem de uma incapacidade de exercício que advém das suas incapacidades psíquica e física. Esta persiste até o cômputo da sua maioridade. No entanto, incapacidade de agir, ao longo dos anos vai se diluindo à medida que o menor adquire maturidade e discernimento para fazer uso dos seus direitos e para atuar de forma responsável. Desta forma, a lei consagrada várias exceções e diferente meios de suprimento pelo instituto da representação.

3. A INTERNET DAS COISAS

A *Internet* foi idealizada na década de 60 para responder, inicialmente, a fins militares. Entretanto, esta rede mundial ganhou protagonismo nas mais variadas áreas sociais, e, hoje, está presente em diversos setores da sociedade, representando um dos elementos imprescindíveis para o seu funcionamento e dinâmica[23].

Como resultado, o avanço da conectividade possibilitou a ampliação da produção e da oferta de novos produtos e serviços, inovação e transformação em diversos campos sociais. Tais progressos desenvolvem-se a passos largos, de tal forma que o Direito nem sempre consegue acompanhar o seu ritmo, refletindo, por vezes, numa regulação deficiente, que se traduz em obstáculos para a plena proteção dos interesses[24] e direitos dos cidadãos, nomeadamente, daqueles que são objeto do nosso estudo: os menores. A rede global trouxe, ainda, uma nova realidade intitulada pelo jurista italiano Stefano

---

[22] Remetemos para carlos Alberto Da Mota Pinto; António J M Pinto Monteiro [et.al.] - *Teoria geral do direito civil*. 5ª ed. Coimbra: Gestlegal, 2020. ISBN: 978-989-8951-53-3. p. 231., que faz, no § IV uma exposição pormenorizada de cada meio de suprimento da incapacidade dos menores.

[23] Manuel Castells - *A sociedade em rede*. 8ª Revista e Ampliada ed. São Paulo: Paz e terra 2005 p. 82-83. "A criação e o desenvolvimento da Internet nas três últimas décadas do seculo XX forma consequência de uma fusão singular de estratégia militar, grande cooperação científica, iniciativa tecnológica e inovação contracultural (...) A primeira rede de computadores (...) entrou em funcionamento em 1º de setembro de 1969..."

[24] Eduardo Magrani - *Entre dados e robôs : ética e privacidade na era da hiperconectividade*. ed. Porto Alegre, RS: Arquipélago Editorial, 2019. ISBN: 9788554500290. p. 15. "Já se sabe qua a tecnologia se desenvolve a largos passos e que o Direito não consegue acompanhar o seu ritmo, de forma que a sua regulação deficiente revela, por vezes, um obstáculo para a plena proteção dos interesses existenciais da pessoa humana. É no âmbito da tecnologia conhecida como Internet das Coisas (ou *Internet of Things,*ou, ainda, IoT) que se revela um dos principais debates nesta área..."

Rodota de "mixed reality[25]", onde as fronteiras do ciberespaço e do mundo físico foram dissolvidas. Esta revolução espacial e conceitual deu origem a um novo ambiente, no qual indivíduos e objetos estão permanentemente interconectados por meio da Internet e interagem entre eles. Neste ecossistema surgiram, como dissemos, as tecnologias da *Internet of Things* ou *Internet das Coisas* (termo que passaremos a utilizar de agora em diante).

3.1. DEFINIÇÃO DE "INTERNET DAS COISAS"

O termo Internet das Coisas foi proposto pela primeira vez em 1999, pelo britânico Kevin Ashton[26]. O referido pesquisador explicou que, tradicionalmente, as tecnologias de computação e comunicação necessitam dos seres humanos para concluir as suas funções. Na prática, é através da digitação, da captação fotográfica e gravação de voz, que os dispositivos armazenam as informações necessárias para desempenhar as suas tarefas. Além disso, Ashton explicou que as pessoas, devido às suas rotinas atarefadas, têm falta de tempo para inserir todos esses dados. Desta forma, os aparelhos deveriam ser capazes de coletar sozinhos tais informações, de modo a conseguirem desempenhar, de forma eficaz, célere e autónoma as suas tarefas e, por conseguinte, facilitar a vida dos seus utilizadores e proporcionar-lhes novas experiências.

Ora, a expressão inglesa *Internet of Things* refere-se, justamente, a estes almejados objetos. As tecnologias pertencentes à Internet das Coisas são, na verdade, objetos do dia a dia, tais como escovas dos dentes, televisores e brinquedos, que são sensíveis à Internet e têm capacidade de coletar, armazenar, processar e comunicar informações sobre si mesmos, dos seus utilizadores e do seu ambiente físico[27]. Em suma, o termo "Internet das Coisas" é a combinação dos elementos de conectividade, autonomia e tratamento de dados que juntos capacitam os objetos "comuns" a desempenharem novas tarefas do dia-a-dia, e, como explicou Kevin Ashton, facilitam a vida dos seus utilizadores.

---

[25] Stefano Rodotà - *Palestra Professor Stefano Rodotà*. In Rio de Janeiro: 2003. 2003. [Consult. 2020-11-25]. Disponível na Internet: <URL: http://www.rio.rj.gov.br/dlstatic/10112/151613/DLFE-4314.pdf/GlobalizacaoeoDireito.pdf>. p. 1-11. O jurista italiano explica que "se olharmos para os processos em curso do ponto de vista das tecnologias da informação e da comunicação, não descobriremos apenas o nascimento de uma dimensão virtual ao lado daquela real, ou formas de misturas que sugerem a expressão *mixed realitiy*."

[26] Eduardo Magrani - *Entre dados e robôs : ética e privacidade na era da hiperconectividade*, cit., p. 30. "Kevin Ashton, do MIT, em 1999, propôs o termo *Internet das Coisas."*

[27] pedro Miguel Pereira Santos - *Internet das coisas: O desafio da privacidade*. Setúbal: Instituto Politécnico de Setúbal 2016. 108 p. Tese de Mestrado. p. V (Resumo). "A Internet das Coisas (...) é o temos utilizado para designar a conectividade entre vários tipos de objetos do dia-a-dia sensíveis à internet, desde eletrodomésticos, carros, roupas, sapatos, remédios, etc., com sensores capazes de captar aspectos do mundo real e enviá-los a plataformas que recebem estas informações e as utilizam de forma inteligente, moldando uma rede de objetos interligados."

3.2. CARACTERÍSTICAS DAS TECNOLOGIAS DA INTERNET DAS COISAS

Segundo o pesquisador Silvo Meira, as tecnologias pertencentes à Internet das Coisas devem comportar, simultaneamente, três características, para serem consideradas um objeto inteligente: capacidade de computação, comunicação e controlo[28].

Tecnicamente, os objetos inteligentes estão equipados com um sistema de radiofrequência em rede (RFID[29]) que os habilita a conectarem-se a uma rede sem fio — comummente à rede Internet — ou a outros objetos inteligentes, através de uma ligação Wi-Fi ou Bluetooth. Esta conectividade cria um novo ambiente onde pessoas e objetos interagem no espaço e no tempo, possibilitando o monitoramento, a manutenção e melhoria do produto. Na prática, ela permite que o utilizador controle remotamente o dispositivo através de uma aplicação e que o operador do sistema faça atualizações no sistema operativo — *software* ou *hardware* — para aprimorar o funcionamento do dispositivo, ou para resolver uma avaria eventual técnica[30]. Ademais, os objetos inteligentes estão equipados com pequenos sensores que possibilitam a comunicação e a realização de funções específicas entre as coisas. Na verdade, eles viabilizam a recolha de dados (como por exemplo, comportamentos, hábitos, imagens, geolocalização, etc.), assim como o armazenamento e tratamento[31] dos mesmos. Uma vez recolhidos e tratados, os dispositivos prestam respostas

---

[28] silvio Meira - Sinais do futuro imediato, #1: internet das coisas. dia a dia, bit a bit [Em linha]. [Consult. 2021-03-13]. Disponível na Internet: <URL: https://silvio.meira.com/silvio/sinais-do-futuro-imediato-1-internet-das-coisas/>. Silva Meira disse que: "a internet das coisas, (...) coisas, aqui, são dispositivos que têm, em alguma intensidade, capacidades de computação, comunicação e controle, simultaneamente ..."

[29] A tecnologia de RFID (do inglês *Radio-Frequency IDentification* – identificação por radiofrequência) é um termo genérico paras as tecnologias que utilizam a frequência de rádio para captura automática e armazenamento de dados. Tecnicamente, as etiquetas ou *tag* RFID são um transporter, isto é, um pequeno objeto colocado num produto que o capacita identificar objetos com dispositivos eletrônicos, que emitem sinais de radiofrequência para leitores que captam estas informações. (Cf. https://www.ncontrol.com.pt/o-que-e-rfid.html [consultado dia 14 de agosto de 2021])

[30] A título ilustrativo podemos citar aquele de "um fabricante de telemóveis inteligentes que, durante a recolha de um dos seus produtos, m 2017, realizou uma atualização de *software* que reduziu a zero a capacidade de bateria dos telemóveis a recolher, para que os utilizadores cessassem a utilização desses aparelhos perigosos". (Cf. *Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica*, COM (2020) 64 final, p. 3).

[31] Donell Holloway E Lelia GreeN - The Internet of toys - *Communication Research & Practice* [Em linha]. Vol: 2, nº 4 (2016), p. 506-506-519. [Consult. 2020-04-14]. Disponível na Internet: <http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=123147016&site=eds-live>. ISSN: 2204-1451 p. 2. "The use of IT technologies to monitor individual children´s online activities already occur at a corporate level and will expand further with Internet-connect toys. Others risks include hacked surveillance of Internet-connected toys, geo-locational tracking of children and remote control of toys various recording and speaking technologies by others".

adequadas e personalizadas em função do perfil e interesses do consumidor. Por fim, Silvo Meira esclarece o quão impreterível é os dispositivos terem as três características — capacidade de computação, comunicação e controlo — simultaneamente. Ele esclarece que se o dispositivo está, apenas, no plano da computação e da comunicação, mas não tem sensores que lhe confiram a característica do controlo, é considerado (apenas) uma máquina em rede. Por outro lado, se o aparelho não possuir a capacidade de comunicação, ele será considerado um sistema de controlo digital. Do mesmo modo, se o objeto não conta com capacidades computacionais, ele é um sistema de telemetria[32].

3.3. TIPOS DE OBJETOS CONECTADOS

Os objetos inteligentes estão presentes no setor público, privado, coletivo e particular. Eles auxiliam na otimização e na autonomização de tarefas básicas do quotidiano e criam novas oportunidades para toda a sociedade global. Progressivamente, eles ganharam — e continuam a ganhar — lugar no nosso espaço de trabalho, influenciam as nossas rotinas, fazem-se presentes nos nossos lares e, até, moldam a maneira como pensamos e nos divertimos. No setor privado, esta nova realidade oferece diferentes funções e cumpre diversos propósitos, como conforto e entretenimento.

Na prática, os consumidores são vastamente beneficiados com a variedade de oferta. Há dispositivos de IdC para casa, vestuário, acessórios, meios de transportes, brinquedos e muito mais. Na verdade, estas novidades tecnológicas são impulsionadas pela demanda massiva que os próprios consumidores causam, em especial, os consumidores-criança[33]. Verdadeiramente, as tecnologias digitais da Internet das Coisas para crianças estão crescendo em peso no mercado global e já são consideradas produto de excelência entre os mais novos. Diariamente, eles são expostos e atraídos ao uso e ao consumo de dispositivos inteligentes. O atual mercado de IdC, separou, especialmente para os menores, produtos inteligentes, como é o caso dos *Smart Toys* (brinquedos inteligentes), relógios conectados para crianças e os monitores de vídeo inteligentes para bebês[34]. Para além destes produtos, os infantes são

---

[32] silvio Meira. cit. O autor define o que para ele são as "coisas", no sentido da expressão internet das coisas. Nessa explicação ele afirma que os dispositivos inteligentes têm que apresentar, "simultaneamente, capacidades de computação, comunicação e controle" caso contrário, o objeto não poderá ser considerado uma "coisa" pertencente a Internet das Coisas.

[33] A categoria jurídica do "consumidor-criança" será abordada no próximo capítulo desta dissertação.

[34] grupo De Trabalho Internacional Sobre Proteção De Dados Nas Telecomunicações - Dispositivos inteligentes para crianças e os riscos para a privacidade. *Forum de proteção de dados*. Lisboa: Comissão Nacional de Protecção de Dados. [Em linha]. Vol: [6 vol.] (2019a) p. 38-49. Disponível na ISSN: 2183-5977. p. 39. "Os dispositivos inteligentes para crianças abrangem os brinquedos inteligentes, os relógios inteligentes, os monitores de bebé e outros dispositivos especificamente destinados às crianças."

imersos e cativados por tecnologias da IdC que, embora não lhe sejam especialmente dirigidas, são objetos com os quais os menores lidam diariamente. Efetivamente, hoje em dia, é comum uma criança ter acesso e usar um *smartphone*[35], ou mesmo alguns dispositivos inteligentes de uso doméstico, como é o caso das "*Smart TV*" (televisões inteligentes).

Posto isto, verificamos que estas inovações tecnológicas estão a lançar vários desafios ao mundo da lei que precisam ser acompanhados, pelo que, julgamos que é necessário o jurista estar familiarizado com a oferta e o funcionamento dos dispositivos de IdC, para assim, estar apto para compreender e desenvolver ferramentas alinhadas e mais assertivas com as necessidades do setor. Por essa razão, dedicaremos as próximas páginas na exposição dos dispositivos destinados e pensados para o consumidor-criança e dos dispositivos inteligentes ofertados aos adultos — ao grande público em geral — mas, como já mencionámos, são regularmente utilizados pelo público infantojuvenil.

a) Dipositivos inteligentes destinados ao "consumidor-criança"

As crianças contemporâneas são consideradas a primeira geração a nascer em lares mediatizados, por conseguinte, são indivíduos familiarizados — embora nem sempre aptos — com o uso dos dispositivos conectados. Os mais novos passam, quotidianamente, uma quantidade significativa do seu tempo consumindo estas tecnologias, o que se tem refletido na maneira como os mais novos pensam, agem, brincam, e até, como eles interagem e encaram o mundo à sua volta[36]. No fundo, os menores são atraídos por um conjunto diversificado de funcionalidades, tais como entretenimento, acesso a informação, meio de interação com amigos e familiares[37]. Diante desta procura, a oferta de IdC para infantes é maioritariamente composta por brinquedos inteligentes e objetos inteligentes de puericultura, que embora não sejam produtos procurados diretamente pelos consumidor-criança, são aparelhos que estão nitidamente e exclusivamente ligados à sua pessoa.

---

35 Tradução para português: telemóveis inteligentes.

36 Sara Pereira - "Os direitos da criança no mundo digital". *Forum de proteção de dados*. cit. p. 10. A professora Sara Pereira aborda a questão da rápida evolução do mundo digital na infância e diz: "O brincar quotidiano é mediado por um conjunto de interfaces tecnológicas, estando estas presente em várias atividades da criança e dos jovens."

37 Grupo De Trabalho Internacional Sobre Proteção De Dados Nas Telecomunicações - Proteção da privacidade das crianças nos serviços em linha. *Forum de proteção de dados*. Lisboa: Comissão Nacional de Protecção de Dados. [Em linha]. Vol: [6 vol.] (2019b) Disponível na ISSN: 2183-5977. p. 51. O documento de trabalho refere no ponto 2. da sua introdução: "Os serviços são utilizados por crianças para uma multiplicidade de propósitos, como por exemplo entretenimento, interação com amigos, familiares e terceiros, consumo de música e vídeos e procura de informação para vários fins, incluindo tarefas escolares."

i. Os brinquedos inteligentes

Uma boneca que conversa com uma criança, um peluche que responde às perguntas que lhe são feitas, um pequeno dinossauro que sabe tudo (ou quase tudo)[38]: estes são apenas alguns dos brinquedos[39], mediados pelo conjunto de interface tecnológica da Internet das Coisas[40], oferecidos no mercado internacional. Mundialmente conhecidos como *smart toys*, proporcionam uma experiência única na infância e uma verdadeira inovação na área do brincar e aprender. Os produtos pertencentes a esta categoria da IdC são essencialmente: tablets, smartphones smartwatches, computadores, câmaras fotográficas, drones[41] e outros aparelhos produzidos especificamente para o consumidor-criança e destinado a ser um brinquedo ou fonte de entretenimento[42].

Na prática, o brinquedo inteligente é concebido para interagir com o consumidor-criança por meio da sua conexão Wi-Fi ou Bluetooth. Para tal, ele é equipado com um sistema de RFDI e sensores, tais como microfones e câmaras, que lhe permite desempenhar funcionalidades especiais, próprias das tecnologias da IdC, como automatização e interatividade. Enquanto produto inteligente, o brinquedo conjuga as três características indispensáveis dos

---

[38] Option Consommateurs - Efants sous écoute La protection de la vie privée dans l'environnement des jouets intelligents 2018. [Consult. 2020-04-22]. Disponível na Internet: <URL: www.option-consommateurs.org>. p. 7. "Une poupée qui discute avec un enfant, un ourson en peluche qui répond aux questions qu'on lui pose, un petit dinosaure qui sait tout (ou presque tout)"

[39] De acordo com as notas introdutórias do Decreto-Lei n.º 43/2011 de 24 de Março, que estabelece as regras de segurança dos brinquedos disponibilizados no mercado, consideramos brinquedo "qualquer produto concedido ou destinado, exclusivamente ou não, a ser utilizado para fins lúdicos por crianças".

[40] Option Consommateurs - *Enfants sous écoute La protection de la vie privée dans l'environnement des jouets intelligents*. cit. p. 7. "Les jouets intelligents sont des objets connectés à Internet avec lesquels l'enfant peut interagir. Grâce à une intelligence artificielle infonuagique, ils permettent le jeu de façon interactive (...) Ces fonctionnalités sont possibles para une collecte à grande echelle de renseignements personnels. En effet, afin de fournir des services "intelligents", ces jouets recueillent une multitude de données à l'aide de microphones, de caméras et d'autres capteurs qui y sont integrés. Ils peuvent enregistrer et transmettre vers des serveurs externes les conversations qu'ils ont avec les enfants ou des données sur leur utilization."

[41] Pequeno avião não tripulado, telecomandado ou programado, frequentemente dotado de aparelho para registo ou transmissão de imagens. (Cf. Dicionário Priberam Online. Disponível em: <https://dicionario.priberam.org/drone> [consultado dia 20 de agosto de 2021].

[42] Rita Brito, Patrícia Dias [et.al.] - Young Children, Digital Media and Smart Toys: How Perceptions Shape Adoption and Domestication - *British Journal of Educational Technology* [Em linha]. Vol: 49, nº 5 (2018), p. 807-820. [Consult. 2020-04-30]. Disponível na Internet: <http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1190597&site=eds-live>. ISSN: 0007-1013 p. 809. "…devices such as tablets, smartphones, smartwatches, computers, cameras, drones and others specifically aimed for children, which are used mainly as toys and sources of entertainment…"

dispositivos inteligentes: capacidade computacional, de comunicação e de comando.[43] Esta conjugação técnica, permite que o menor interaja e controle remotamente o brinquedo, através de um telemóvel inteligente, um Tablet, ou ainda, por estímulos de voz, emissão de sons e reação a comandos externos tal como a fala e movimentos corporais. Complementarmente, ele é, ainda, supervisionado e monitorado pelo seu produtor, que, à distância, pode efetuar atualizações no seu sistema operativo, para aperfeiçoar e incrementar novas funcionalidades, e assim, melhorar o produto e zelar pela sua segurança.

A oferta de brinquedos inteligentes no mercado internacional é rica e diversificada. Todavia, o consumo de IdC para crianças, em Portugal, encontra-se numa fase embrionária. Mesmo assim, um estudo feito com famílias portuguesas[44], aferiu que muitas das nossas crianças conhecem vários dos brinquedos inteligentes disponíveis no mercado internacional e mostraram interesse em obter ou pelo menos experimentá-los[45]. Embora a oferta seja reduzida, ou quase inexistente, encontramos alguns IdC para crianças em interfaces comerciais situadas em Portugal, como por exemplo, na *FNAC* e na *Worten.*

Nesses termos, iremos, portanto, afunilar o nosso estudo na exposição de dois brinquedos comercializados nas mencionadas lojas: o Tablet "tab4you" da "Iki Mobile" e o relógio "Kids Watch 4G" da "Innjoo". A intenção da nossa exposição é entendermos quais as funcionalidades que os brinquedos oferecem às crianças para, de seguida, discutirmos os eventuais riscos que estes produtos podem causar nas suas vidas.

O "tab4you" da "Iki Mobile":

O famoso "tab4you" foi o primeiro Tablet infantil produzido em Portugal[46]. Como qualquer dispositivo conectado, o "tab4you" tem capacidade compu-

---

43 Quanto as características *vide supra* Silvio Meira. *cit. (*ponto 3. do presente capítulo)

44 Rita Brito [et.al.]. cit. p. 807-820. O estudo concentra-se no consumo das tecnologias digitais na infância, das crianças portuguesas, olhando especialmente para brinquedos inteligentes.

45 Rita Brito [et.al.]. cit. p. 817. A pesquisa da Dra. Rita Brito, publicada no British Journal of Educational Technology, está relacionado com tecnologias educacionais digitais e quais os seus impactos sociais. O estudo realizado revelou que muitas crianças portuguesas já pediram aos pais brinquedos inteligentes, todavia, alguns pais não adquiriam por causa de vários fatores, entre eles: "a barrier mentioned by some parents is the high price of the smart toys. Some elaborate that they need to consider if the child is going to play with the toy for a long time, if the toy is going to bring the child satisfaction and entertainment and also if the toy is educational, or if they are going to spend a lot of money in a toy that the child will be bored with after a short time…". Outro ponto relevante que o referido estudo apresentou foi a diferença socio-económica do agregado familiar "…in Portugal, the smart toys market is still in an early stage. We found some early adopters of smart toys, but were scarce, even in homes with high penetration of digital devices and in families with high incomes.

46 Ele é fabricado pela empresa de telemóveis Iki Mobile e distribuído pela empresa *"Science4you"*. Este aparelho pode ser adquirido por um preço compreendido entre 100€ a 120€, dependendo do modelo, e é destinado a crianças na faixa etária dos 8 aos 13 anos.

tacional, de comunicação e de controlo através dos seus sensores, inclusive de RFDI, que faz ligação à Internet por meio de ligação Wi-Fi. Atualmente, o modelo 7 do "tab4you" (o mais avançado, à data de hoje), está equipado com o sistema operativo Android 9.0.

O "tab4you" promete funcionalidades distintas, entre elas, o divertimento pelo intermédio de jogos (alguns previamente instalados e com capacidade para instalar outros), e por meio de aplicações que já estão previamente instaladas, como "Mundo do Panda", "Zooky Find" e "ZookkyLand MoneyMouse", e também funcionalidades educativas, como por exemplo, o aparelho é comercializado com um livro educativo eletrónico, e foi especialmente pensado e produzido para servir de instrumento de apoio escolar ao longo do ano letivo da criança. Adicionalmente, o Tablet comporta duas câmaras, uma frontal e outra traseira, e, por meio delas, a criança pode tirar fotografias e fazer filmagens, e ainda usá-las como meio responsivo para jogos e outras aplicações. Por fim, a sua ligação à rede Internet abre um leque de oportunidades para o consumidor-criança, uma vez o que possibilita aceder conteúdos online, comunicar com outras pessoas, ver vídeos, e muito mais.

"Kids Watch 4G" da "Innjoo":

Os relógios inteligentes são brinquedos inteligentes para crianças, que integram o grupo das "tecnologias vestíveis", mais conhecidas por "*Smart Wearable Devices*" (termo em inglês), os quais se referem a dispositivos que podem ser usados no corpo, como acessórios e roupas. Na prática, eles auxiliam na saúde, na segurança e promovem entretenimento ao seu utilizador. Não há dúvidas que as tecnologias vestíveis representam uma das mercadorias de maior expansão no mercado tecnológico português. Nos últimos anos, elas desenvolveram-se em quantidade — com uma oferta mais diversificada — e em qualidade — com aperfeiçoamento e implemento de novas funcionalidades[47]. Além do mais, elas tornaram-se mais acessíveis monetariamente, com uma redução significativa dos seus preços. Tudo isto levou a um acréscimo notável da sua procura pelos consumidores portugueses. Atualmente, a subcategoria mais popular das tecnologias vestíveis são os relógios inteligentes ("*SmartWatches"* — termo em inglês) e as pulseiras desportivas (também conhecidas como "*SmartBands"* — termo em inglês), que fazem sucesso entre os consumidores, inclusive face aos consumidores-crianças. Tecnicamente, os relógios inteligentes, graças aos

[47] vivian Genaro Motti - "Wearable Technologies: a Roadmap to the Future". *WebMedia'20: Proceedings of the Brazilian Symposium on Multimedia and the Web*. [Em linha]. (2020) p. 3-4. [Consult. 2021-03-19]. Disponível na Internet: <URL: https://dl.acm.org/doi/pdf/10.1145/3428658.3431928>. ISSN: 978-1-4503-8196-3. p. "Wearable technologies have a large potential to amplify human abilities. Thanks to their close contact to the human body, their miniaturized dimensions and continuous data collection, wearables are versatile, meeting system requirements across domains. Wear- able technologies have grown in quantity and quality over the past decades, gaining popularity".

seus biossensores[48], são capazes de, em tempo real, detetar, diagnosticar, monitorar e comunicar informações sobre a saúde e o desempenho físico do seu utilizador, através da recolha de dados pessoais, legalmente considerados como sensíveis[49], como por exemplo, a frequência cardíaca, e a temperatura corporal.

Em Portugal, encontramos facilmente relógios inteligentes que foram pensados e desenhados para crianças, como é o caso da *Kids Watch 4G*[50], da empresa Innjoo. Atualmente, os relógios inteligentes são considerados a tecnologia vestível mais popular entre os infantes. O *Kids Watch 4G*, para além de indicar as horas, tem funcionalidades de comunicação, monitoramento e entretenimento[51].

A função de comunicação possibilita ao menor efetuar e receber chamadas de voz e de vídeo; enviar e receber mensagens de voz e de texto e assim, comunicar com amigos, familiares e com os pais. Ademais, o relógio está habilitado a registar contactos e receber um cartão Nano SIM, apresentando-se como um verdadeiro meio de comunicação móvel.

Por sua vez, a função de monitoramento desempenha várias funções. Em primeiro lugar, e, provavelmente, a funcionalidade mais aclamada pelos progenitores, o relógio permite, que a situação do menor seja monitorada, em tempo real, através de um sistema de geolocalização integrado, de forma a assegurar que a criança se encontra numa situação de normalidade[52]. Tecnicamente, ela indica a localização exata do menor, graças a sua funcionalidade de "*precise positioning*" e pelo viés de uma aplicação chamada "SeTracker 2"[53]. Em segundo lugar, o dispositivo possui um botão lateral de SOS[54] que corrobora para a segurança do infante. Esta função foi pensada para

---

48 São sensores que detetam movimento, temperatura corporal ou recorrem a um organismo vivo —por exemplo o coração — para detetar batimentos cardíacos, movimento ou temperatura e os converter em sinais eletrónicos, aos quais chamamos de dados sensíveis.

49 O jurista Eduardo Magrani define dados sensíveis como "informações que podem ser utilizadas de forma discriminatória e, portanto, carecem de proteção especial, como aqueles sobre a origem racial ou étnica de um indivíduo; suas convicções religiosas; filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político; sobre sua saúde ou vida sexual; e dados genéticos e biométricos." (Cf. *Entre dados e robôs : ética e privacidade na era da hiperconectividade*, cit., p. 57)

50 Vende-se em lojas como a Fnac, a um preço considerado acessível (entre 110,00€ a 130,00€) e também em sites como: https://udi.pt/produto/smartwatch-innjoo-kids-watch-4g-azul/ (acedido dia 17.03.21).

51 Vide *Reloj Inteligente para niños de Innjoo*. [Vídeo]. Realização de WWWHATSNEW. 2020. Disponível na Internet: <URL: https://www.youtube.com/watch?v=iwXGo3yQp3Q>.

52 Na prática, os representantes legais instalam a aplicação num dispositivo inteligente — geralmente no seu "*smartphone*" pessoal — que possibilita o rastreamento do menor.

53 É uma aplicação que está disponível para sistemas operativos Android e IOS. Para mais informações, pode ser consultada em: < https://play.google.com/store/apps/details?id=com.tgelec.setracker&hl=pt_PT&gl=US > [consultado dia 3 de agosto de 2021]

54 *Apresentação Smart Watch Infantil 4G, Wi-Fi e Bluetooth Relógio infantil GPS, Monitoramento Remoto*. [Vídeo]. Realização de MOSTRAÊ! 2019. Disponível na Internet: <URL: https://www.youtube.com/watch?v=wBPYhKGTCLw>.

assistir a criança numa eventual situação de perigo, que, ao carregar no botão enviará um sinal de alerta para o número de telefone de urgência associado, desta forma, o responsável poderá localizar, através da aplicação, o posicionamento geográfico exato do menor, acionar a camara do relógio e os seus sensores de áudio[55], para comunicar com o infante — para dar-lhe assistência, por exemplo — ouvir e visualizar o ambiente no qual a criança se apresenta. Simultaneamente, o sistema de monitoramento habilita os responsáveis legais a delinear uma área geográfica na qual a criança poderá locomover-se livremente[56]. No entanto, se o menor se afastar ou sair da zona previamente configurada, o sistema notificará[57] os responsáveis de uma possível situação de risco da sua criança. Adicionalmente, o sistema de geolocalização — por intermédio do "*history tracking*" — permite registar os lugares onde a criança esteve e quais ela frequenta diariamente, nomeadamente a sua morada, o seu estabelecimento escolar, desportivo, cultural, etc.[58]. Por último, a funcionalidade de monitoramento auxilia no acompanhamento do bem-estar vital da criança. De facto, o *Kids Watch 4G* tem capacidade para medir e coletar, em tempo real, por intermédio dos seus biossensores, dados sensíveis do menor, como por exemplo, o seu ritmo cardíaco[59] e até mesmo a sua temperatura[60]. Para além disso, os biossensores do Kids Watch 4G induzem, indiretamente, a criança a praticar atividade física. O relógio regista a quantidade de passos que o menor dá por dia [61], consequentemente, incentiva a criança a completar metas diárias, o que ajuda, por exemplo, a travar o sedentarismo infantil.

Por fim, a função de entretenimento oferece divertimento ao menor. Por um lado, por meio da sua câmara frontal "HD Photo" [62], o relógio permite que as crianças tirem fotografias e façam filmagens para registar momentos com os seus amigos e familiares. Por outro lado, o relógio está habilitado a

---

55 Pode-se ligar a camara ou os sensores de áudio remotamente, a partir da aplicação, sem mesmo que a criança saiba, ou se dê conta que os seus representantes legais estão a ouvir ou ver aquilo que ela está fazendo ou dizendo.

56 Pelo viés da sua função "*Electronic Fence".*

57 Défenseur Des Droits - Monde Numérique: Quels Droits? In droits - *Educadroit - Manuel d'éducation au Droit* [Em linha]. Défenseur des droits, [Consult. 2021-03-02]. p. 17. Disponível na Internet: <URL: https://educadroit.fr/sites/default/files/Manuel-Education-au-Droit-2020-chap11.pdf>. "Les montres connectées présentent généralement les fonctionalitées suivantes: Communiquer avec l'enfant (messagerie, téléphone); Savoir précisément où est situés l'enfant, avec une alerte s'il s'écarte du chemin de l'école ou d'une zone déterminée; Mesurer em temps réel la santé de l'enfant, grâce à des capteurs (rythme cardiaque); Encourager l'enfant à faire du sport, à se dépenser , grâce à um traceur d'activité (nombre de pas); Divertir l'enfant avec des fonctions de prise de photo, des jeux et des applications."

58 Défenseur Des Droits, cit., p. 4. *Vide* nota anterior.

59 Défenseur Des Droits, cit., p. 4. *Vide* nota 54.

60 *Apresentação Smart Watch Infantil 4G, Wi-Fi e Bluetooth Relógio infantil GPS, Monitoramento Remoto*. cit.

61 Défenseur Des Droits, cit., p. 4..

62 *Apresentação Smart Watch Infantil 4G, Wi-Fi e Bluetooth Relógio infantil GPS, Monitoramento Remoto*. cit.

ter jogos, como é o caso de um jogo de matemática que já vem previamente integrado no produto.

ii. Objetos inteligentes de puericultura

Sem dúvidas, o nascimento de uma criança é um acontecimento repleto de desafios e dificuldades para os pais, que procuram sempre zelar pela saúde e o bem-estar do seu filho. Tendo em conta estas dificuldades, as novas tecnologias da IdC têm sido desenvolvidas para auxiliar os representantes legais. Neste sentido, embora os aparelhos de puericultura sejam destinados a ser utilizados pelos pais, são produtos pensados e produzidos para serem usados direitamente com bebés. Da mesma forma, eles são desenvolvidos para cumprir, sobretudo, funções de vigilância, mas também para acompanhar o desenvolvimento e o estado de saúde dos bebés.

Como qualquer dispositivo inteligente, os objetos inteligentes de puericultura estão equipados com um sistema operativo, sensores e têm ligação à Internet, que possibilita o desempenho das suas funções, nomeadamente, controlo remoto do aparelho através de smartphones, Tablet, e em alguns casos, no próprio computador.

Atualmente, o mercado das tecnologias de IdC na área de puericultura é composta maioritariamente por monitores de vídeo para bebés, berços e até mesmo tecnologias vestíveis, como por exemplo um "smart body"[63]. No entanto, o produto mais adquirido pelos pais são os monitores de vídeo. Estes são verdadeiras "babás eletrónicas[64]", uma vez que auxiliam os responsáveis com várias funcionalidades, entre elas, vigilância, comunicação, monitorização da respiração, da temperatura e até mesmo do sono do recém-nascido.

Para a nossa exposição, iremos destacar um dos mais recentes monitores de vídeo para bebés, o "Miku Pro Smart Baby Monitor"[65] da empresa norte-americana Mikucare. Este monitor de vídeo está equipado com uma câmara de vídeo que permite vigiar a criança a qualquer momento do dia, inclusive enquanto esta dorme, em qualquer lugar, pois basta conectar-se por ligação Internet ao aparelho, através da sua aplicação, que poderá ver (e ouvir) o cenário em que a criança está inserida. Além disso, poderá rever gravações que a câmara regista ao longo do dia e da noite. O "Miku Pro" também tem microfones e altifalantes que possibilitam uma conversa direcional entre o

---

63 O "Mimo" é um body para bebés de 0 a 12 meses. Esta tecnologia vestível é concessionada para vigiar, ininterruptamente, os dados de saúde do recém-nascido, tais como temperatura, respiração e sono. O facto de se conectar com outros dispositivos inteligentes, nomeadamente, os sm*artphones*, permite que os pais possam aceder a tais informações a qualquer momento e em qualquer lugar do mundo, bastando estarem conectados à Internet. Disponível em https://www.youtube.com/watch?v=n2TUMA3IaIU [acedido dia 10 de agosto de 2021]

64 Termo utilizado no Brasil para referir-se a monitores de vídeo para bebés.

65 Disponível em: < https://mikucare.com/ > [acedido 10 de agosto de 2021]

bebé e os seus pais. Ademais, o aparelho tem sensores capazes de medir a temperatura da criança, a humidade do espaço, a intensidade do som e da luz do ambiente no qual a criança está inserida, para, assim, assegurar de forma constante, o bem-estar do menor. Adicionalmente, o aparelho consegue, em tempo real, rastrear padrões de respiração e de sono do bebé. Todas as informações recolhidas pelo produto podem ser consultadas a qualquer momento do dia, e mais, em qualquer lugar do mundo, através da aplicação "Miku Baby Monitor"[66]. Por último, o aparelho está programado para emitir alertas, relacionados com anomalias na respiração ou no sono da criança, assim como avisar os pais do seu despertar, movimentos e sons, como por exemplo, o choro. Ademais, com os dados sensíveis recolhidos, os cuidadores (representantes legais e mesmo os médicos) podem analisar a saúde e o desenvolvimento da criança.

b) Dipositivos inteligentes para o consumidor adulto

Além dos produtos inteligentes destinados ao consumidor-criança, há, no tráfego jurídico, inúmeros dispositivos da IdC destinados ao consumidor adulto. Embora eles não sejam pensados e produzidos diretamente para o consumo juvenil, os menores tornaram-se os consumidores mais assíduos destas tecnologias, apesar de nem sempre estarem preparados para o seu uso correto e seguro.

Diferentemente do consumo de brinquedos inteligentes, o lar português, hodiernamente, adquire cada vez mais tecnologias pertencentes à Internet das Coisas, porém para o uso doméstico. Frente a este cenário, a criança portuguesa inicia a sua experiência com as IdC, dentro do seu próprio agregado familiar, e, não raras as vezes, como vimos *supra*, desde o seu nascimento[67]. Na verdade, é mais comum encontrarmos em Portugal uma criança que tenha acesso e consuma, diariamente, um dispositivo de uso doméstico, como é o caso das "Smart TVs" do que um brinquedo inteligente. Por estes motivos, julgamos relevante analisar dispositivos inteligentes que são ofertados ao grande público, uma vez que as crianças são sensivelmente expostas a estes todos os dias, no seu espaço seguro, no seu lar. Neste sentido, elegemos as "Smart TVs", pois acreditamos, que é o aparelho conectado de uso doméstico mais consumido em Portugal.

i. Televisão inteligente

Há muitos anos que a televisão é o principal objeto de diversão no seio de várias famílias, nomeadamente, da família portuguesa. Para além do mais, o atual período pandémico devido à COVID-19, levou as famílias a passarem

---

66 Disponível em: < https://mikucare.com/pages/privacy-policy >[Consultado dia 11 de agosto de 2021]

67 Como por exemplo, com o uso de monitores de vídeo para bebés.

muito mais tempo em casa[68] e, por conseguinte, o consumo de televisão ascendeu consideravelmente, e com ele, o aperfeiçoamento, o desenvolvimento e a oferta de novos televisores, conhecidos como "Smart TVs". A expressão inglesa "Smart TVs" é, como dissemos, traduzida para o português como televisões inteligentes ou televisores conectados. Como a sua designação denuncia, estes aparelhos são, tecnicamente, a junção de uma televisão clássica com um sistema operativo que permite ao utilizador manusear o aparelho como se se tratasse de um verdadeiro computador, em troca de uma experiência interativa e personalizada[69], típica das tecnologias da IdC.

Em Portugal, podemos adquirir televisões inteligentes que oferecem funcionalidades tais como: acessar à Internet, instalar e usufruir de diversas aplicações como *Netflix*, *Disney+*, *YouTube*, *Spotify*, *Facebook*, aplicações de jogos e muito mais. Alguns televisores inteligentes têm sensores como câmaras, microfones e altifalantes embutidos que potencializam os períodos de lazer, e personalizam a experiência do seu utilizador. Ademais, os microfones e altifalantes permitem que o consumidor comande a sua televisão com comando de voz, e ainda, realizar diversas funções por intermédio da sua assistente virtual[70] embutida, como consultar a meteorologia ou controlar outros dispositivos inteligentes do lar.

Claramente, as crianças ficam encantadas diante de tais funcionalidades. De acordo com a última pesquisa realizada pela ERC (Entidade Reguladora para a Comunicação Social) no ano de 2017, 94% das crianças portuguesas, entre os três e os oito anos, viu programas televisivos todos os dias ou quase[71]. Embora o estudo tenha relatado que apenas 26% usou um televisor in-

---

[68] carla Bernardino - "2020 sentou mais 350 mil portugueses por dia em frente à TV. A maioria a pagar" [Em linha]. *Diário de Notícias*. [Consult. 2021-09-14]. Disponível na Internet: <URL: https://www.dn.pt/edicao-do-dia/03-jan-2021/2020-sentou-mais-350-mil-portugueses-por-dia-em-frente-a-tv-a-maioria-a-pagar-13188007.html>."O consumo televisivo disparou em um ano de pandemia, com mais de 196 mil espectadores a pagar para ver conteúdos no pequeno ecrã [...] O recolhimento para todos e o isolamento profilático e a quarentena para muitos empurraram os portugueses para o sofá e para os ecrãs. Em 2020, foram mais de 349 mil pessoas por dia a assistir televisão…"

[69] *TechNews: Sistema operacional LG webOS une tecnologia e uma experiência completa - #JM*. [Vídeo]. Realização de NEWS, Jovem Pan. 2021. Disponível na Internet: <URL: https://www.youtube.com/watch?v=KtHhriDH75c>.

[70] Uma assistente virtual utiliza inteligência artificial (IA) para identificar e responder comandos de voz. Ela permite realizar funções diversas, como solicitar informações, controlar itens da casa e criar próprias rotinas. Com o comando de voz, é possível criar uma conversa com a IA, com respostas inteligentes e adaptadas para cada usuário e ainda realizar diferentes solicitações. (Cf. https://canaltech.com.br/software/google-assistente-o-que-e/ [acedido dia 20 de agosto de 2021]).

[71] Cristina Ponte, José Alberto Simões [et.al.] - *Estudo crescendo entre ecrãs - Usos de meios eletrónicos por crianças (3-8 anos).* 2017. [Consult. 2021-02-22]. Disponível na Internet: <URL: https://www.erc.pt/documentos/Crescendoentreecras/mobile/index.html#p=1>. p. 30. No ano de 2017, "A quase totalidade das crianças de três a oito anos (94%) vê programas televisivos todos os dias ou quase, sem grande variação por sexo

teligente, estatísticas mais recentes apontam que, só no primeiro trimestre do ano de 2019, "aparelhos como Smart TV crescem 12,3% em Portugal"[72]. Decerto que o número de televisores inteligentes prosseguiu com o seu acentuado crescimento e, subsequentemente, o infante português é diariamente exposto a este tipo de produto.

Por último, vale relembrar que todo o dispositivo inteligente produz efeitos importantes e interdependentes na vida das crianças e nos seus direitos, mesmo quando elas não são consumidoras diretas, ou seja, os menores não precisam necessariamente utilizar os dispositivos inteligentes para que a conectividade dos aparelhos à Internet afete os seus direitos.

4. CATEGORIA JURÍDICA DE *"CONSUMIDOR-CRIANÇA"*

Incontestavelmente, as tecnologias pertencentes à Internet das Coisas integram o conjunto de produtos de eleição dos atuais consumidores, e as crianças representam, dentro da bolha desta indústria, um mercado altamente lucrativo[73]. Como já tivemos a oportunidade de ver *supra,* há exclusivamente para os menores, uma vasta oferta de produtos e serviços inteligentes concebidos para satisfazer as suas necessidades e interesses. Diante deste cenário, as crianças apresentam-se como verdadeiras consumidoras, e, por conseguinte, são titulares de direitos e garantias no âmbito do direito do consumidor. No entanto por se apresentarem como entes frágeis e vulneráveis, as crianças são colocadas numa especial posição de consumo.

ou idade. Apenas três inquiridos indicaram que a criança não via televisão. Aos dias de semana, a média de visionamento é de 1:41 hora, entre um mínimo de meia hora e um máximo de cinco horas. Nos dias de fim-de-semana, sobe para 2:51 horas, entre o mínimo de meia hora e o máximo de oito horas." Todavia, ressalvamos que, por conta da pandemia COVID-19, e o seu consequente confinamento social, as crianças nos últimos dois anos tiveram muito mais expostas ao visionamento televisivo, elevando os números apresentados consideravelmente.

[72] João Tomé - *Aparelho como a Smart TV crescem 12,3% em Portugal. Samsung lidera.* 2019. [Consut. 2021-08-05]. Disponível na Internet: <URL: https://insider.dn.pt/em-rede/aparelhos-como-a-smart-tv-crescem-123-em-portugal-samsung-lidera/19452/ >.

[73] Ohana Trajano Barbosa e Andres Rodriguez Veloso - Vulnerabilidade da Criança no Varejo: Um Estudo Sob a Perspectiva da Pesquisa Transformativa do Consumidor - *GESTÃO.Org: Revista Eletrônica de Gestão_Organizacional* [Em linha]. Vol: 15, nº 1 (2017), p. 1-1-10. [Consult. 2021-03-29]. Disponível na Internet: <https://periodicos.ufpe.br/revistas/gestaoorg/article/download/23042/24610>. ISSN: 1679-1827 p. 1. Nesse sentido, os autores explicam que "As crianças representam um mercado altamente lucrativo sendo constantemente alvo como qualquer outro mercado consumidor, das práticas de marketing, propagandas e táticas de vendas."

4.1. DEFINIÇÃO JURÍDICA DE CONSUMIDOR-CRIANÇA

O ordenamento jurídico português consagra um estatuto especial dos consumidores. Embora, entre nós, não haja um conceito único de consumidor, nós podemos encontrar, em diferentes diplomas normativos (inclusive aqueles que não tenham sido vocacionados para regulamentar, especificamente, matéria do consumo) uma noção ampla relativamente ao seu âmbito teleológico[74]. Dentre os diplomas normativos vigentes, destacamos, desde logo o n.º 1 do art. 60.º da CRP que elenca os direitos do consumidor: "Os consumidores têm direito à qualidade dos bens e serviços consumidos, à formação e à informação, à protecção da saúde, da segurança e dos seus interesses económicos, bem como à reparação de danos." Revemos estes direitos consagrados na Lei n.º 24/96, de 31 de julho, que estabelece o regime legal aplicável à defesa dos consumidores. Ademais, esta lei dá-nos a definição mais relevante de consumidor[75]. Ela considera consumidor "todo aquele a quem sejam fornecidos bens, prestados serviços ou transmitidos quaisquer direitos, destinados a uso não profissional, por pessoa que exerça com carácter profissional uma atividade económica que vise obtenção de benefícios" (n.º 1, art. 2.º). Segundo Jorge Morais Carvalho, o conceito de consumidor consagrado neste preceito é bastante amplo[76]. Para ele, a noção é muito mais complexa do que uma estrita posição contratual. De facto, o conceito de consumidor alarga-se aos sujeitos que irão consumir e utilizar o produto, sem, contudo, o terem necessariamente adquirido. Verdadeiramente, o n.º 1, art. 2.º da Lei n.º 24/96, não assume nenhuma presunção de capacidade de exercício para celebrar autonomamente um negócio jurídico, tão-pouco há instauração de um pré-requisito de capacidade negocial[77]. Dito isto, e tendo em consi-

---

74 Jorge Morais Carvalho - *Manual de Direito do Consumo* Ed. 2013. Isbn: 978-972-40-5377-6. P. 12-13. "como não existe um conceito único, a nível nacional e internacional, é necessário perceber em cada caso qual o âmbito subjetivo de aplicação do diploma em causa. Integram a esfera do direito de consumo muitas normas que não têm o consumidor como referência para delimitação do seu âmbito de aplicação (...) Estamos, assim, perante normas de direito do consumo que não têm por referência (apenas) o consumidor, qualquer que seja o conceito adotado".

75 Jorge Morais Carvalho - *Manual de Direito do Consumo* cit., p. 13.

76 Para Jorge Morais Carvalho - *Manual de Direito do Consumo* cit., p. 13-18, o conceito de consumidor pode ser analisado com referência a quatro elementos: o subjetivo, o objetivo, o teleológico e o relacional.

77 Diógenes Faria De Carvalho e Thaynara De Souza Oliveira - "A categoria jurídica de 'consumidor-criança' e sua hipervulnerabilidade no mercado de consumo brasileiro". *Revista Luso-Brasileira de Direito do Consumo* [Em linha]. Vol: V N.º 17 (2015) p. 207-230. [Consult. 2020-03-20]. Disponível na Internet: <URL: https://app.vlex.com/#vid/561354770>. p. 215. Nesse sentido os autores explicam que "... o conceito de consumidor extrapola em muito os sujeitos da relação, quem, como a criança, utiliza o produto ou serviço sem, contudo, tê-lo adquirido), ressai manifesto que o conceito jurídico de consumidor não exclui a figura da criança, meramente por esta não possuir capacidade de facto para celebrar negócio jurídico".

deração o atual panorama consumista no qual as crianças contemporâneas ocupam uma posição de suma relevância, defendemos que os menores são tidos como verdadeiros consumidores, pois, além de lhes serem destinados bens e serviços, eles consomem e utilizam os produtos inteligentes disponíveis no mercado, mesmo que não tenham, para isso, ocupado, uma posição contratual na relação de consumo.

Efetivamente, não há dúvidas que, devido à crescente oferta de produtos destinados às crianças, à influência das suas preferências que direcionam as tendências[78] do consumo de bens e serviços do seu agregado familiar, os menores devem, definitivamente, ser incluídos no âmbito conceitual e teleológico do art. 2.º da Lei n.º 24/96. Tal abrangência, deu origem a uma nova categoria jurídica denominada consumidor-criança[79].

Na verdade, esta elasticidade do conceito de consumidor tem vindo a ser adotada pela jurisprudência portuguesa, nomeadamente já no Acórdão da Relação do Porto de 11/09/2008[80], que determinou que a noção de consumidor tem de ser atualizada na medida em que não só sofre de algumas imprecisões e insuficiências, como não pode deixar de ser completada, nomeadamente, com elementos de cariz sociológico. De facto, as transformações tecnológicas têm influência no direito do consumo, e, por conseguinte, impactam as esferas jurídicas dos consumidores. Hoje em dia, o conceito de consumidor sofreu uma expansão conceitual, abraçando as crianças como verdadeiras consumidoras. Consequentemente, o consumidor-criança, tal como todos os consumidores, é protegido pelas disposições gerais e especiais que regulam o direito do consumidor.

4.2. A VULNERABILIDADE AGRAVADA DO CONSUMIDOR-CRIANÇA

Segundo o pai da produção em série, Henry Ford, o consumidor é "o elo mais fraco da economia"[81]. Neste sentido, os instrumentos de políticas dos consumidores visam proteger todos os consumidores nas suas relações com os comerciantes profissionais. Entende-se que todos os consumidores são

---

[78] Juliet B. Schor - *Nascidos para comprar: uma leitura essencial para orientarmos nossas crianças na era do_consumismo*. 1ª ed. São Paulo: Editora Gente, 2009. ISBN: 978-85-7312-570-2. p. 2.

[79] Diógenes Faria De Carvalho [et.al.] - "A categoria jurídica de 'consumidor-criança' e sua hipervulnerabilidade no mercado de consumo brasileiro". *Revista Luso-Brasileira de Direito do Consumo* cit. p. 2.

[80] Acórdão da Relação do Porto, de 11/09/2008, Processo n.º 0834643, do Relator Fernando Baptista. Disponível na Internet em: <http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df538025758300 4ee7d7/ce7cfdb89c941f62802574da0053e534?OpenDocument>

[81] Diógenes Faria De Carvalho [et.al.] - "A categoria jurídica de 'consumidor-criança' e sua hipervulnerabilidade no mercado de consumo brasileiro". *Revista Luso-Brasileira de Direito do Consumo* cit. p. 216.

geralmente parte mais fraca numa transação[82] e por isso merecem uma proteção e regulamentação especial devido à sua debilidade oriunda de um desequilíbrio em termos económicos, educacionais e de poder aquisitivo, face à outra parte da relação de consumo, o profissional. Em harmonia, o direito português reconhece a vulnerabilidade do consumidor, e como resultado, o nosso ordenamento jurídico dispõe de um rico catálogo normativo composto por normas de fonte externa[83] e interna, entre elas disposições constitucionais[84] e legislação ordinária de caracter geral e especial[85].

Contudo, denota-se que certos grupos de consumidores podem, em determinadas situações, ser particularmente vulneráveis e necessitar de salvaguardas específicas. De facto, a vulnerabilidade do consumidor pode ser definidas em função de determinadas circunstâncias ou de características específicas de consumidores individuais ou de grupos de consumidores, tais como a idade, o género, a saúde, a literacia digital, a numeraria ou a situação financeira[86]. Efetivamente, destacamos aqui, em especial, a posição do consumidor-criança, que devido à sua especial situação jurídica de menoridade, merece uma proteção reforçada. No fundo, os menores têm dificuldades em compreender e avaliar autonomamente a relação de consumo. De acordo com um estudo realizado por Wided Batat[87], a vulnerabilidade do consumidor-criança dá-se por vários fatores. Entre eles destacamos a impulsividade do menor ao consumo, o facto de eles, no geral, não conseguirem resistir à pressão de grupo, nem perceberem como os dispositivos inteligentes podem impactar os seus direitos e como tais influências podem ter implicações na sua vida adulta. Neste sentido, não há dúvidas que os consumidores-crianças

---

82 COM(2020) 696 final - *Nova Agenda do Consumidor - Reforçar a resiliência para uma recuperação sustentável* Bruxelas 2020b. Disponível na Internet: <URL: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=COM:2020:696:FIN>.

83 A título de exemplo citamos um diploma comunitário, a Diretiva 2001/95/CE, relativa à segurança geral dos produtos.

84 Artigo 60.º (Direitos dos consumidores) da Constituição da República Portuguesa.

85 Já tivemos a oportunidade e citar pontualmente a Lei da Defesa do Consumidor, mas há muitos outros diplomas especiais que regulam, direta e indiretamente os direitos dos consumidores. Por exemplo, nós iremos *infra*, estudar o Decreto-Lei n.º 69/2005, de 17 de marco, relativamente à segurança geral dos produtos. Sem dúvidas que este documento normativo, indiretamente, protege em grande escala, a esfera jurídica dos consumidores. De facto, regular sobre a segurança dos produtos e serviços colocados no mercado constitui um elemento fundamental de garantia do respeito pelos direitos dos consumidores consagrados na Constituição e na lei, com especial destaque para o direito à proteção da saúde e da sua segurança física. (Cf. Sumário do D-L n.º 69/200, disponível em https://dre.pt/pesquisa/-/search/574566/details/maximized, consultado dia 18 de agosto de 2021).

86 COM(2020) 696 final - *Nova Agenda do Consumidor - Reforçar a resiliência para uma recuperação sustentável* Bruxelas 2020b.

87 Wided Batat - Comment les adolescents définissent-ils leurs propres compétences en matière de consommation ? Une approche par les portraits - *Recherche et Applications en Marketing (French Edition)* [Em linha]. Vol: 29, nº 1 (2014), p. 27-60. Disponível na Internet: <https://journals.sagepub.com/doi/abs/10.1177/0767370113505946>. p. 27-28.

estão numa posição de maior debilidade em relação à vulnerabilidade reconhecida no consumidor-padrão.

Efetivamente, como definiram os autores Diógenes Faria de Carvalho e Thaynara de Souza Oliveira, o consumidor-criança sofre de uma vulnerabilidade agravada[88], ou, como intitulam no ordenamento jurídico brasileiro, de hipervulnerabilidade[89]. Contudo, esta especial debilidade toma uma proporção significativa face ao consumo das tecnologias das IdC, que expõem os mais novos a situações especiais de perigo, nomeadamente, situações relacionadas com falhas de segurança que teremos a oportunidade de estudar no próximo capítulo.

Ora, devemos, no entanto, ter em consideração que vulnerabilidade agravada é uma presunção, que não pode ser tida como absoluta, e sim relativa.

a) A vulnerabilidade agravada relativa

O reconhecimento da presunção de vulnerabilidade para todos os consumidores não significa, contudo, que eles sofrem do mesmo nível de vulnerabilidade perante o fornecedor[90]. Há diferenças entre os consumidores que se refletem no grau da sua vulnerabilidade, tal como o seu conhecimento acerca das tecnologias, a sua idade, a sua profissão (que pode estar relacionada ou nitidamente ligada ao uso de dispositivos tecnológicos, por exemplo), o seu nível económico e social, etc. De facto, "o próprio conceito genérico de consumidor vai perdendo a sua funcionalidade em determinados contextos de uso nos quais se torna necessária uma distinção entre tipos de consumidor[91]".

Realmente, tal diferenciação é nítida no âmbito do uso e consumo das tecnologias da IdC. É inegável que há utilizadores mais "experientes" do que outros, e por isso, entre os consumidores, não podemos tratar da questão da vulnerabilidade como uma presunção geral e absoluta. Tem de haver um tratamento *in concreto,* isto é, temos de ter em consideração a situação do consumidor em causa.

Nesta lógica, o mesmo se aplica à categoria jurídica de consumidores-crianças. Há crianças mais ou menos experientes do que outras, e consequentemente,

---

88 Diógenes Faria De Carvalho [et.al.] - "A categoria jurídica de 'consumidor-criança' e sua hipervulnerabilidade no mercado de consumo brasileiro". *Revista Luso-Brasileira de Direito do Consumo* cit. p. 208-209.

89 Diógenes Faria De Carvalho [et.al.] - "A categoria jurídica de 'consumidor-criança' e sua hipervulnerabilidade no mercado de consumo brasileiro". *Revista Luso-Brasileira de Direito do Consumo* cit. p. 218.

90 Diógenes Faria De Carvalho [et.al.] - "A categoria jurídica de 'consumidor-criança' e sua hipervulnerabilidade no mercado de consumo brasileiro". *Revista Luso-Brasileira de Direito do Consumo* cit. p. 220.(Nesse sentido cfr. MIRAGEM, Bruno, *Curso do direito do consumidor*p.100-101).

91 Nesse sentido cfr. Diógenes Faria De Carvalho [et.al.] - "A categoria jurídica de 'consumidor-criança' e sua hipervulnerabilidade no mercado de consumo brasileiro". *Revista Luso-Brasileira de Direito do Consumo* cit. p. 221.

a presunção da vulnerabilidade agravada irá variar consoante o grau de fragilidade do menor, seja por conta da sua idade, conhecimento, meio social, etc.

Entre nós, idêntico critério parece ter sido adotado no âmbito da capacidade de agir do menor. Efetivamente, tal como já tivemos a oportunidade de ver *supra,* o menor carece de uma incapacidade de exercício (art. 123.º CC) atrelada à sua especial situação de menoridade. Nas palavras de Mota Pinto, a capacidade de exercício refere-se à aptidão para agir sozinho, o que supõe uma capacidade natural de querer e entender. É por esta razão que os menores são considerados incapazes, pois eles não conseguem determinar, com normal esclarecimento ou liberdade interior os seus interesses[92], e por isso, é-lhes imposta a incapacidade de exercício para prática da maioria dos seus atos.

Porém, ao mesmo tempo que o art. 123.º do CC estabelece a regra geral da incapacidade de exercício, o preceito também admite exceções. Efetivamente, aquando da sua redação, o legislador civil decidiu incluir a expressão "salvo disposição em contrário"[93]. "Desta forma, o caráter padronizado da fixação da maioridade do décimo oitavo aniversário é atenuado pela lei, à medida que o menor vai adquirindo capacidade por patamares etários[94]".

Entre as várias exceções consagradas[95], encontramos logo no art. 127.º do CC as "exceções mais importantes e mais significativas[96]" para atenuação da incapacidade de exercício. Nestes casos o legislador pressupõe que o menor já possui o discernimento e o poder de avaliação suficientes para agir em conformidade com os seus interesses e para assumir as respetivas responsabilidades, e confere assim, alguma flexibilidade àquela solução. A *ratio* desta elasticidade reside no facto da maturidade e do discernimento — dois pressupostos imprescindíveis para a determinação da capacidade de exercício — não se adquirirem de modo instantâneo, mas sim gradual[97]. Dentro

---

92 carlos Alberto Da Mota Pinto; António J M Pinto Monteiro [et.al.] - Teoria geral do direito civil, cit., p. 196-197. Nesse sentido o professor Mota Pinto, referindo a capacidade de exercício, diz que a aptidão para agir supõe uma capacidade natural de querer e entender. Por isso, quem, por falta de experiência mediana não possa determinar com normal esclarecimento ou liberdade interior os seus interesses, devem estar desprovidas de capacidade de exercício.

93 heinrich Ewald Horster - *A parte Geral do Código Civil Português - Teoria Geral do Direito Civil* 2ª ed. Coimbra: Almedina, 2019. ISBN: 978-972-40-8146-5. p. 322.

94 Pedro Pais De Vasconcelos - *Teoria geral do direito civil* 6ª ed. ed. Coimbra 2010. ISBN: 978-972-40-4369-9. p. 112

95 Para além das exceções à incapacidade consagrada no art. 127º, outras estão previstas no CC, com por exemplo, nos arts. 1289º, n.º 2 (capacidade para adquirir por usucapião), no art. 1957, n.º (convocação do conselho de família). Há outras exceções consagras em vários diplomas normativos, como é o caso do art. 8.º do Regulamento Geral de Proteção de Dados, que estatui a capacidade para consentimento de em relação aos serviços da informação para 16 anos.

96 heinrich Ewald Horster - *A parte Geral do Código Civil Português - Teoria Geral do Direito Civil* cit., p. 322

97 heinrich Ewald Horster - *A parte Geral do Código Civil Português - Teoria Geral do Direito Civil* cit., p. 322. Além do referido, Heinrich Horster explica ainda que a lei tem

do corpo do art. 127.º, consideramos que al. b) do n. º1 é o preceito que apresenta o maior grau de flexibilidade, quando estatui "os negócios próprios da vida corrente do menor que, estando ao alcance da sua capacidade natural, só impliquem despesas, ou disposições de bens, de pequena importância" pois ele permite fazer face a uma grande diversidade de situações, atendendo ao respetivo caso concreto. Esta alínea faz "coincidir a capacidade de exercício com a capacidade natural. Reconhece-se, assim, capacidade ao menor para os atos que estejam ao alcance da sua maturidade, discernimento e experiência.[98]".

Deste modo, há diferenças entre os consumidores-criança. Estas variações refletem-se no grau da vulnerabilidade do menor, isto é, há crianças mais ou menos aptas ao uso e consumo dos dispositivos inteligentes, e por isso, face às tecnologias da IdC, devemos ter em conta vários critérios, tais como a idade, o nível de educação escolar e tecnológica, por exemplo, para a determinação da vulnerabilidade agravada do consumidor-criança. Na verdade, além da idade, devemos também ter em consideração o nível de instrução e conhecimento que o menor tem face às tecnologias, assim como a sua aptidão em usar e consumir os dispositivos inteligentes[99]. Adicionalmente, o usual contacto que o infante tem com as tecnologias da IdC, o seu meio sociocultural e socioeconómico também são determinantes para avaliação da fragilidade do menor perante produtos conectados.

Dito isto, concluímos que não podemos tratar da questão da vulnerabilidade agravada como uma presunção geral e absoluta. Tem de haver um tratamento *in concreto*, consoante o grau de fragilidade do menor, consoante, em suma, a sua "capacidade natural".

4.3. DIREITOS DO CONSUMIDOR-CRIANÇA NO DIREITO PORTUGUÊS

A proteção dos consumidores é garantida por meio de vários diplomas normativos. No âmbito do direito interno, destacamos a Constituição da República Portuguesa, através do seu artigo 60.º, cujo desenvolvimento legislativo é levado a cabo pela Lei n.º 24/96, de 31 de julho, que estabelece o regime legal aplicável à defesa dos consumidores.

---

de considerar as exigências da segurança do tráfico jurídico, mas também tem que ter em consideração à autodeterminação e auto-regulamentação da pessoa, na medida que ela se torna cada vez mais responsável.

98 Pedro Pais De Vasconcelos - Teoria geral do direito civil cit., p. 115.

99 Nas suas orientações políticas, a Presidente da Comissão Europeia sublinhou a necessidade de desenvolver competências digitais para todos. O Plano de Ação para a Educação Digital 2021-2027 (COM (2020) 624 final – Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Bruxelas: 2020) determinou que a tecnologia digital se tornou essencial para a vida quotidiana de todos, inclusive das crianças. Acrescentou ainda que, quando as tecnologias são utilizadas de forma eficiente, equitativa e eficaz, elas contribuem para que todos sejam bem sucedidos num mundo em rápida evolução e os permite adaptar-se as novas e emergentes tecnologias, inclusive, aquelas que pertencem à IdC.

Os direitos dos consumidores estão consagrados — no quadro jurídico interno e geral de proteção dos consumidores — nos art. 60.º da CRP e art. 3.º da Lei n.º 24/96, de 31 de julho, a saber, eles têm direito: à qualidade dos bens e serviços; à proteção da saúde e da segurança física; à formação e à educação para o consumo; à informação para o consumo; à proteção dos interesses económicos; à prevenção e à reparação dos danos patrimoniais ou não patrimoniais que resultem da ofensa de interesses ou direitos individuais homogéneos, coletivos ou difusos; à proteção jurídica e uma justiça acessível e pronta; e à participação, por via representativa, na definição legal ou administrativa dos seus direitos e interesses[100].

5. OS PRODUTOS INTELIGENTES E AS SUAS FALHAS DE SEGURANÇA

Hoje em dia, uma criança no aconchego do seu lar pode sofrer situações de perigo ocasionadas por falhas de segurança relacionadas com dispositivos inteligentes presentes no seu agregado familiar, os quais, direta ou indiretamente, põem em risco a vida do seu utilizador e perturbam os seus direitos. No fundo, os impactos negativos provenientes do ambiente conectado são cada vez mais comuns, e por isso, não podem ser desvalorizados. Pelo contrário, devemos reunir todos os esforços necessários para que os direitos, as liberdades e as garantias das crianças sejam assegurados em qualquer situação e em qualquer lugar, inclusive, no ambiente digital.

Neste espírito, cabe-nos, no presente capítulo, demostrar quais são as fontes — no ambiente conectado — que jorram riscos e ameaças para os direitos dos menores e quais as suas respetivas consequências. Desta forma, entenderemos que os produtos da IdC colocam novos desafios no atual quadro normativo em matéria de segurança dos produtos e em termos de responsabilidade. Por conseguinte, interpretaremos o quadro normativo do Decreto-Lei n.º 383/89, de 6 de novembro, relativo à responsabilidade decorrente de produtos defeituosos, à luz do mercado tecnológico contemporâneo.

5.1. AS FONTES DAS FALHAS DE SEGURANÇA NOS PRODUTOS INTELIGENTES E AS SUAS CONSEQUÊNCIAS

Nos últimos tempos, têm-se registado várias situações de perigo com menores, relacionadas com falhas de segurança provenientes de dispositivos inteligentes, nomeadamente, brinquedos, relógios para crianças e Smart TVs. Face às frequentes anomalias, peritos em segurança e várias associa-

[100] Para mais desenvolvimento sobre estes direitos ver David Falcão - *Lições de Direito do Consumo* [Em linha]. 2ª Edição ed. Coimbra: Almedina, 2020. [Consult. 2021-09-07]. Disponível na Internet: <URL: https://ebooks.almedina.net/reader/books/9789724094168>. ISBN 978-972-40-9416-8. p. 25-49.

ções europeias dos consumidores[101] realizaram testes em diferentes dispositivos que revelaram a existência de falhas de segurança preocupantes[102]. Se outrora era comum os progenitores alertarem os seus filhos para não falarem com estranhos na rua, hoje em dia, esta advertência, perdeu significado. De facto, os resultados dos testes revelaram que a maioria das falhas possibilitavam um estranho comunicar-se — inclusive sem violar o funcionamento do sistema operativo[103] do aparelho — com uma criança por intermédio de aparelhos conectados. Na prática, o terceiro conseguiria enviar áudios, ou ainda, intercetar, remotamente, conversas que estivessem a decorrer junto ao dispositivo.

Há cerca de cinco anos, houve um caso de grande repercussão no norte da Europa relacionado com falhas de segurança de uma boneca inteligente, a "My Friend Cayla", da empresa Genesis. Tecnicamente o defeito do brinquedo possibilitava que um desconhecido utilizasse o seu microfone e os seus altifalantes como viés de comunicação com a criança[104]. Além disso, qualquer pessoa que tivesse a aplicação da boneca instalada no seu dispositivo (telemóvel inteligente ou Tablet), detetaria, à sua proximidade, uma boneca "My Friend Cayla", isto porque, a conexão Bluetooth do brinquedo não podia ser desligada, nem ser protegida através de um sistema de senhas. Tais fatores conduziram à proibição da comercialização do brinquedo na Alemanha, e levaram as autoridades alemãs a retirar a boneca de circulação[105]. Além disso, houve uma recomendação emitida para os consumidores, mais especificamente para os pais, para desligarem o brinquedo permanentemente.

Outro incidente similar ocorreu recentemente na Islândia, o qual levou as autoridades islandesas a apresentarem uma notificação ao Sistema de Troca Rápida de Informação da UE (RAPEX)[106]. Neste caso, a falha de segu-

---

101 Em causa, estamos a referir, especificamente as associações do Reino Unido, da Bélgica, da Alemanha e da Espanha. Vide Grupo de Trabalho Internacional sobre Proteção de Dados nas Telecomunicações - Dispositivos inteligentes para crianças e os riscos para a privacidade. *Forum de proteção de dados*. cit. p. 39.

102 *Vide* nota anterior.

103 Marina Pita - Brinquedos conectados e os riscos à infância. Politics. Instituto Nupef. [Em linha]. (2019) p. 19-40. Disponível na Internet: <URL: https://politics.org.br/sites/default/files/downloads/nupef_politics29_web.pdf>. ISSN: 1984-8803. p. 19-40.

104 Option Consommateurs - Efants sous écoute La protection de la vie privée dans l'environnement des jouets intelligents. cit. p. 15. "Le cas le plus fréquemment rapporté est celui de la poupée *My Friend Cayla*, produite par Genesis, dont les vulnérabilités pourraient donner l'occasion à un pirate d'utiliser son microphone pour parler à distance avec l'enfant".

105 Mafalda Miranda Barbosa - Obrigação geral de segurança e responsabilidade civil. *Estudos de Direito do Consumidor.* Coimbra Faculdade de Direito Universidade de Coimbra [Em linha]. Vol: 14 (2018) p. 273-341. Disponível na ISSN: 1646-0375. p. 299. Note-se que, de acordo com o artigo 6.º n.º 4 do DL n.º 69/2005, a recolha do produto, enquanto medida adequada, fica submetida a critérios de necessidade e subsidiariedade. Assim ela deve ter lugar sempre que as outras ações — informar sobre os riscos e retirar os produtos do mercado — não forem suficientes para fazer face aos riscos.

106 O RAPEX (*rapid alert system for non-food dangerous products*) é um sistema europeu de alerta rápido para produtos perigosos de natureza não alimentar colocados

rança provinha de um relógio inteligente para crianças[107], que, tal como o "Kids Watch 4G", tinha funcionalidades de comunicação e monitorização do menor por intermédio de um sistema de geolocalização. Afigurou-se, no entanto, que o relógio permitia que os seus consumidores fossem localizados e contactados, por qualquer pessoa, inclusive pelas autoridades islandesas, que, facilmente, conseguiram localizar todos os utilizadores, intercetar as suas conversas, e ainda conversar com os consumidores-crianças[108].

Face ao exposto, é inegável afirmar que os dispositivos inteligentes põem em risco diferentes direitos de personalidade dos mais novos. Segundo Scott R. Peppet[109], as falhas de segurança nos produtos da IdC e os consequentes ataques informáticos ocorrem por três motivos.

A primeira razão que Scott apresenta está relacionada com questões técnicas. Ele explica que a maioria das atuais empresas que atuam no mercado das tecnologias da IdC não são especializadas em desenvolvimento de *software* ou *hardware* de alto nível, mas sim na produção de bens de consumo "comuns". Deste modo, a falta de conhecimento e experiência em matéria de segurança traduz-se numa incompetência que se reflete na produção e na oferta de produtos defeituosos a nível computacional.

O segundo argumento apresentado pelo teórico, aborda o aspeto físico do objeto. Usualmente, as tecnologias inteligentes têm uma estrutura compacta (um *smartwatch* por exemplo) que dificulta o espaço nos objetos para

no mercado que contribui para a garantia do respeito pelos direitos dos consumidores, com especial destaque para o direito à proteção da saúde e da sua segurança física. Autoridade de Segurança Alimentar e Económica - *RAPEX (Rapid Alert System for all dangerous consumer Products)* [Em linha]. [Consult. 2021-08-21]. Disponível na Internet: <URL: https://www.asae.gov.pt/inspecao-fiscalizacao/sistemas-de-alerta-e-troca-de-informacao/rapex.aspx>. Ademais, neste sentido,Mafalda Barbosa explica que o RAPEX visa garantir que os produtos perigosos sejam rapidamente retirados de circulação, prevenindo a consumação dos riscos que eles envolvem para o consumidor. (Cf. Mafalda Miranda Barbosa - Obrigação geral de segurança e responsabilidade civil. *Estudos de Direito do Consumidor.* cit. p. 300-302.).

[107] Notificação RAPEX da Islândia, publicada no sítio WEB "Safety Gate" da UE. *EUROPEAN COMMISSION - Alert number: A12/0157/19* [Em linha]. Germany: European Commission. [Consult. 2021-08-06]. Disponível na Internet: <URL: https://ec.europa.eu/safety-gate-alerts/screen/webReport/alertDetail/349994>.

[108] Manon Flausch - *Rapex, le système européen garant de la sécurité des produits* [Em linha]. EURACTIV.fr. [Consult. 2021-08-06]. Disponível na Internet: <URL: https://www.euractiv.fr/section/soci-t/news/rapex-le-systeme-europeen-garant-de-la-securite-des-produits/?_ga=2.113835584.679216804.1628262614-947037014.1628262614>.

[109] Scott R. Peppet - "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent" - *Texas Law Rewiew* [Em linha]. Vol: 93:85, nº (2014), p. 78. Disponível na Internet: <https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf>. p. 133-135. O autor aponta quatro problemas oriundos da IdC, entre eles, Scott fala sobre a segurança. Dentro desta área ele subdivide em mais dois "the technical problem: Internet of Things devices may be inherently prone to security flaws" e "The legal problem: data security law is unprepared".

suportar um sistema de processamento de dados eficiente e seguro. Além disso, alguns dispositivos inteligentes são tão pequenos, que a sua bateria não tem potência suficiente para processar sistemas de segurança de dados complexos.

Por último, o professor de Direito explica que a maioria das IdC, apesar de serem, na prática, verdadeiros computadores, não são desenvolvidas para serem frequentemente atualizadas, e, por conseguinte, são incapazes de aprimorar os seus sistemas de segurança de dados, tornando-se rapidamente obsoletas, suscetíveis a ataques informáticos e brechas para intromissões indevidas na vida das crianças.

Além dos motivos apresentados pelo jurista norte-americano, a Comissão Europeia (CE) elaborou, no ano passado, um relatório sobre as implicações em matéria de segurança do produto e de responsabilidade decorrentes da inteligência artificial, da Internet das Coisas e da robótica[110]. Neste documento, a Comissão enumerou dois desafios colocados pelas novas tecnologias, inclusive pelos dispositivos inteligentes, que põem em causa o conceito tradicional de segurança, a saber: a conectividade e a complexidade dos objetos inteligentes.

Relativamente à conectividade, como já vimos *supra,* é uma das características fundamentais dos objetos inteligentes. Ela possibilita que o aparelho se ligue à rede Internet e a outros objetos. Segundo a Organização "Internet Society" a expressão "Internet das Coisas" é a extensão da conectividade de rede e capacidade de computação para objeto, dispositivos, sensores e outros artefactos[111]. No fundo, esta funcionalidade abre uma porta para um novo mundo: o mundo "online". Por meio deste espaço, ao mesmo tempo que se consegue retirar e oferecer muitas oportunidades para os consumidores, também se põe em causa o conceito tradicional de segurança. Eduardo Magrani afirmou: "Tudo o que é conectado é vulnerável"[112]. De facto, a conexão à Internet pode comprometer direta e indiretamente a segurança

---

[110] COM(2020) 64 final - *Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica*. Bruxelas: 2020a. Disponível na Internet: <URL: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0064&from=PT>.

[111] Internet Society - *C'est quoi un appareil de l'IdO?* [Em linha]. Internet Society. [Consult. 2021-02-22]. Disponível na Internet: <URL: https://www.internetsociety.org/fr/iot/>. "C'est un objet qui se connecte à Internet. Il peut s'agir d'un pisteur fitness, d'un thermostat, d'une serrure ou d'un appareil — même une ampoule."

[112] Eduardo Magrani - "Tudo o que é conectado é vulnerável". *Internet das coisas e inovação* [Em linha]. [Consult. 2020-11-23]. Disponível na Internet: <URL: http://eduardomagrani.com/tudo-que-e-conectado-e-vulneravel-diz-pesquisador/>.Numa entrevista, onde o pesquisador Magrani abordou as dificuldades e os benefícios da IdC, especificamente no Brasil, o autor afirmou que "Tudo que é conectado é vulnerável. As pessoas não atualizam o software, não cuidam da segurança, não trocam senhas. É preciso entender o problema de segurança como algo muito próximo".

dos produtos e por conseguinte, afeta a segurança dos seus utilizadores[113], em especial os consumidores-criança, que por força da sua natural fragilidade e imaturidade não conhecem os limites de navegação.

Como já foi afirmado: "... o Tablet oferece à criança uma porta aberta para Internet... [114]". De facto, quando uma criança navega na Internet, ela expõe-se a um ambiente onde ocorrem várias ameaças direcionadas a lesar os seus direitos que poderão, inclusive, ter graves repercussões, quer no presente, quer na sua vida adulta. Na prática, através da sua conectividade, os dipositivos inteligentes, como por exemplo, o "tab4you" — como todos os Tablets[115] — pode, rapidamente, tornar-se um caminho fácil para a realização de crimes de natureza sexual, como por exemplo pornografia, prostituição, tráfico de seres humanos, aliciamento de menores, exploração sexual e abuso sexual[116] [117]; mas também crimes relacionados com ofen-

---

[113] COM (2020) 64 final – Relatório as Comissão ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu – *Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52020DC0064 >

[114] *Tab4you 6 é um Tablet Made in Portugal | Reportagem Futuro Hoje SIC*. [Vídeo]. Realização de SCIENCE4YOU. 2019. Disponível na Internet: <URL: https://www.youtube.com/watch?v=Z7RF40PNVVI&t=22s>. O apresentador Lourenço Medeiros, referindo-se ao "tab4you" disse: "Oferecer um Tablet é oferecer uma porta para a Internet e a ter responsabilidade, bom senso e acompanhamento das crianças."

[115] Cristina Ponte [et.al.] - *Estudo crescendo entre ecrãs - Usos de meios eletrónicos por crianças (3-8 anos).* cit. p. 62. Num estudo realizado pela ERC procurou-se identificar os ambientes de ecrãs em que vivem as crianças (dos 3 aos 8 anos), os seus modos de acesso e usos, como os pais orientam esses usos e as suas atitudes e preocupações. Relativamente ao acesso e uso da internet, ficou provado que "o *tablet* é o dispositivo mais usado para a criança ir à internet, referido por 63% dos inquiridos cujas crianças acedem à rede".

[116] Manuel Magriço - "A Internet e as crianças - riscos e potencialidades". *In Judiciários - Coleção formação contínua: jurisdição da família e das crianças* [Em linha]. Lisboa: 2018. [Consult. 2021-08-03]. p. 9-32. Disponível na Internet: <URL: http://www.cej.mj.pt/cej/recursos/ebooks/familia/eb_InternetCriancas2018.pdf>. ISBN: 978-972-9122-98-9. "Segundo dados disponíveis do Conselho da Europa, cerca de uma criança em cinco na Europa é vítima de alguma forma de violência sexual (...) pode assumir muitas formas, tais como o incesto, pornografia, prostituição, tráfico de seres humanos, aliciamento pela internet, exploração sexual e abuso sexual. Todas elas podem causar, e causam, graves danos à saúde mental e física das crianças. As consequências do abuso sexual prolongam-se até à vida adulta das crianças – os seus testemunhos na primeira pessoa mostram que a tristeza e a dor continuam a acompanhá-las secretamente ao longo de toda a sua vida".

[117] Destacamos que, durante o confinamento devido a COVID-19, o número de casos de abuso sexual de crianças, na União Europeia, aumentou consideravelmente. A comissária europeia dos Assuntos Internos, Ylva Johansson disse que "é uma questão muito importante, que tem vindo [...]a crescer exponencialmente [...] durante a pandemia, os pedófilos passavam mais tempo na internet". O total de casos de abuso sexual de crianças reportados às autoridades na Europa passou de 23 mil em 2010 para 725 mil em 2020. (Cf. Lusa – *Abuso sexual de crianças na UE aumentou durante o confinamento*, Jornal Público Online, 24 de julho de 2020. Disponível em <https://www.publico.pt/2020/07/24/sociedade/

sa à integridade física e contra a liberdade pessoal dos infantes. Note-se que, infelizmente, entre nós, esta realidade é bastante comum. Somente no ano de 2018, em média, uma em cada cinco criança europeias, reportou ter tido situações que a incomodou na Internet, como por exemplo, exposição a conteúdos pornográficos ou violentos, contactos inapropriados, ou vítima de comportamentos agressivos[118]. Embora as infrações sejam, na maioria das vezes de âmbito penal, há outros tipos de lesões de direitos, como os ilícitos de âmbito civil, por violação de direitos de personalidade (art. 70.º do CC), como o direito à reserva sobre a intimidade da vida privada (art. 80.º do CC), de âmbito comunitário, e.g., tratamento ilícito dos dados pessoais dos menores (arts. 6.º e 8.º do RGPD[119]), etc.

Posto isto, percebemos que um Tablet com acesso à internet, ou uma boneca que desempenha as suas funcionalidades por intermédio da sua conexão à rede, são exemplos de produtos que, padecendo de falhas de segurança, serão, certamente, fontes de violação e ameaças de direitos dos menores.

Paralelamente, a perda da conexão pode, do mesmo modo, ser fonte de riscos para comprometer a segurança dos menores. *Supra*, quando elencámos os objetos inteligentes para crianças, vimos que entre as várias funcionalidades que o "Kids Watch 4G" desempenha, o relógio permite que o menor acione um botão de SOS para alertar os seus pais de uma eventual situação de perigo. Ora, a falta de conetividade no relógio impedirá que a notificação do pedido de ajuda chegue aos progenitores, que, consequentemente, não ficarão a par da situação de perigo, e, por conseguinte, não prestarão auxílio ao seu filho.

Outro exemplo de caráter mais geral — apresentado pela CE[120] — é o caso de um alarme de incêndio conectado perder a sua ligação e, por esta razão, não alertar o utilizador quando necessário. Desta situação, podem ocorrer danos patrimoniais e não patrimoniais, inclusive na esfera jurídica de crianças envolvidas.

Por último, a CE apontou uma fonte de riscos ligada à complexidade dos produtos e dos sistemas das tecnologias da IdC. A nosso ver, esta fonte pode ser estudada através de três aspetos. Os dois primeiros referem-se à complexidade da composição tecnológica dos produtos inteligentes. Por sua vez, o terceiro aspeto diz respeito à essência daquilo que é a Internet das Coisas.

Em primeiro lugar, como é sabido, o produto final das IdC é a junção de vários outros produtos. Na prática, o produtor constrói o produto final com

---

noticia/abuso-sexual-criancas-ue-aumentou-durante-confinamento-1925705> [Acedido dia 20 de agosto de 2021])

118 *Vide* nota 116.

119 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoas e à livre circulação desses dados.

120 COM(2020) 64 final - *Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica*. Bruxelas: 2020a.

peças (que, por sua vez, também são produtos) provenientes de diferentes fornecedores, prestadores de serviços e distribuidores. Esta complexidade da cadeia produtiva poderá gerar problemas de teor técnico, e.g., incompatibilidades entre as ditas peças, que poderão danificar o produto final e, consequentemente, comprometer o funcionamento seguro, fiável e coerente do aparelho. Ademais, a junção de diversos produtos e intervenientes no processo produtivo, poderá desencadear dificuldades relacionadas com o apuramento da origem do problema, i.e., colocará novos desafios em matéria de proteção dos consumidores e responsabilidade do produtor.

Por sua vez, o segundo aspeto está associado a uma componente essencial para o funcionamento do dispositivo: o *software* ou o *hardware* do produto. Efetivamente, o produto pode sofrer falhas de segurança advindas de posteriores atualizações feitas no sistema operativo, ou mesmo pela falta delas. Do mesmo modo, as atualizações de *software* podem alterar significativamente o produto, introduzindo novos riscos não previstos na avaliação inicial, tão-pouco aquando da sua disponibilização no mercado[121].

Por último, o terceiro aspeto diz respeito ao âmago da Internet das Coisas. Os dispositivos inteligentes são desenvolvidos para se interligarem com vários aparelhos e criarem, desta forma, um ecossistema interligado, onde encontramos dispositivos provenientes de diferentes produtores, programadores e distribuidores. Face a tal enredo, torna-se difícil garantir a plena segurança do produto, uma vez que, basta um dispositivo, nesta teia interligada, apresentar alguma falha para corromper a segurança de um ou de vários outros objetos interligados.

Em conclusão, afirmamos que as tecnologias pertencentes à Internet das Coisas comportam riscos — provenientes de diferentes fontes — associados a danos sobre interesses juridicamente protegidos. Face a esta "multiplicação dos acidentes de consumo"[122] provenientes dos produtos inteligentes, é essencial determinar se, e em que medida, os mencionados diplomas em matéria de segurança e de responsabilidade continuam a ser adequados para proteger os utilizadores das IdC, em especial, as crianças que estão particularmente expostas aos riscos relacionados com os produtos. De todos os produtos notificados como perigosos no sistema de alerta rápido (RAPEX) em 2019, 32% eram brinquedos ou produtos para crianças. Este

[121] Relativamente a questão *software* do produto, teremos a oportunidade de detalhar mais a frente.

[122] Juliana Campos - "A responsabilidade civil do produtor pelos danos causados por rôbos inteligentes à luz do regime do Decreto-Lei n.º 383/89, de 6 de novembro". *Revista de Direito da Responsabilidade* [Em linha]. Vol: ANO 1 (2019) p. 700-730. [Consult. 2021-08-21]. Disponível na Internet: <URL: https://revistadireitoresponsabilidade.pt/2019/a-responsabilidade-civil-do-produtor-pelos-danos-causados-por-robos-inteligentes-a-luz-do-regime-do-decreto-lei-n-o383-89-de-6-de-novembro-juliana-campos/>. ISSN: 2184-4542. p. 705.

dado mostra que as crianças representam um grupo de consumidores mais vulneráveis em termos de segurança de produtos[123].

5.2. O QUADRO NORMATIVO EM MATÉRIA DE SEGURANÇA GERAL DOS PRODUTOS E RESPONSABILIDADE OBJETIVA DO PRODUTOR

O atual quadro normativo, em matéria de segurança do produto e de responsabilidade objetiva do produtor, visa assegurar que todos os produtos colocados no mercado cumpram elevados requisitos de segurança, para proteger os direitos dos consumidores. Efetivamente, tanto o art. 5.º da Lei 24/96, de 31 de julho, bem como os Decretos-Lei 69/2005, de 17 de março e o 383/89, de 6 de novembro, que dizem respeito, respetivamente, às garantias de segurança dos produtos e serviços colocados no mercado e à responsabilidade objetiva do produtor decorrente de produtos defeituosos, contribuem para a concretização da obrigação geral de segurança do consumidor[124]. Todavia, a transformação digital está a mudar radicalmente a vida dos consumidores, e por isso, tendo em conta o ritmo acelerado do progresso tecnológico e do seu impacto na experiência dos consumidores, é necessário tomar medidas adicionais[125]. Ora, os referidos diplomas foram em grande parte estabelecidos antes da emergência das novas tecnologias, pelo que, nem sempre contêm disposições explícitas relativas aos novos desafios do ambiente conectado, levando à redução da sua eficácia.

Diante do exposto, a Comissão Europeia ao mesmo tempo que declarou a superveniência de lacunas decorrentes dos avanços tecnológicos e científicos, também determinou que a neutralidade do regime jurídico — do ponto de vista tecnológico — não implica que o atual quadro não se possa aplicar a produtos da IdC[126]. Adicionalmente, a CE afirmou que as vítimas de acidentes relacionados com produtos e serviços que utilizam novas tecnologias digitais não devem beneficiar de um nível de proteção inferior ao das vítimas de acidentes relacionados com outros produtos e serviços semelhantes.

Neste sentido, iremos agora, especificamente, confrontar o regime especial da responsabilidade do produtor decorrente de produtos defeituosos, consagrado no Decreto-Lei n.º 383/89, de 06 de novembro[127], com o intuito de analisar e enunciar quais as adaptações que, a nosso ver, devem ser observadas, de modo a que os direitos dos consumidores no ambiente conectado sejam

---

123 COM(2020) 696 final - *Nova Agenda do Consumidor - Reforçar a resiliência para uma recuperação sustentável* Bruxelas 2020b.

124 David Falcão - Lições de Direito do Consumo, cit., p. 29.

125 COM(2020) 696 final - *Nova Agenda do Consumidor - Reforçar a resiliência para uma recuperação sustentável* Bruxelas 2020b.

126 COM(2020) 64 final - *Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica*. Bruxelas: 2020a.

127 O qual foi alterado pelo Decreto-Lei n.º 131/2001, de 24 de abril que transpôs a Diretiva 1999/34/CE, de 10 de maio de 1999.

assegurados, em especial, os direitos do consumidor-criança, que à custa da sua vulnerabilidade agravada, tem dificuldades em detetar os riscos oriundos da complexidade dos produtos inteligentes.

a) A aplicação do Decreto-Lei n.º 383/89, de 6 de novembro aos danos causados ao menor por dispositivos inteligentes

De um modo geral, o consumidor não possui conhecimentos necessários para fazer prova da ação ou omissão ilícita e culposa do produtor que provoca danos na sua esfera jurídica[128]. Assim sendo, Portugal acautelou a vulnerabilidade do consumidor no Decreto-Lei n.º 383/89, de 6 de novembro, que transpõe para a ordem jurídica interna a Diretiva 85/374/CEE, de 25 de julho de 1985, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados membros em matéria de responsabilidade por produtos defeituosos. Todavia, o referido decreto-lei foi aprovado quando os dispositivos conectados eram raros. Esta evolução põe em causa a atual definição de produtos e introduz novos riscos ou altera a forma como os riscos existentes se podem concretizar.

No seu primeiro artigo, está consagrado que o "produtor é responsável, independente de culpa, pelos danos causados por defeitos dos produtos que põe em circulação". Assim, entende-se que a responsabilidade objetiva é o meio adequado para resolver o problema da "justa atribuição dos riscos inerentes à produção técnica moderna, na esteira da "strict products liability"[129]. Efetivamente, tal como relatou Moreira Alves, tinha de "existir uma responsabilidade que, ultrapassando a fronteira da culpa, garanta os mais diversos e frequentes riscos" associados à produção defeituosa, "em homenagem à segurança social de todos e cada um dos cidadãos"[130], inclusive a produção defeituosa de produtos inteligentes. Assim, todo o produto defeituoso, dispo-

---

128 Vera Lúcia Paiva Coelho - Responsabilidade do produtor por produtos defeituosos "Teste de resistência" ao DL n.º 383/89, de 6 de novembro, à luz da jurisprudência recente, 25 anos volvidos sobre a sua entrada em vigor. *Revista Eletrónica de Direito* Porto Faculdade de Direito Universidade do Porto [Em linha]. Vol: N.º 2 (2017) p. 1-54. Disponível na Internet: <URL: https://cije.up.pt/pt/red/edicoes-anteriores/2017-nordm-2/responsabilidade-do-produtor-por-produtos-defeituosos-ldquoteste-de-resistenciardquo-ao-dl-nordm-38389-de-6-de-novembro-a-luz-da-jurisprudencia-recente-25-anos-volvidos-sobre-a-sua-entrada-em-vigor/>. ISSN: 2182-9845. p. 27 "E isso acontece porque o lesado não tem os conhecimentos que são necessários para fazer cabalmente essa prova, não domina o modo de fabrico ou de conceção do produto, desconhece a sua composição, as partes componentes, as matérias primas, as informações, instruções ou advertências que integram ou deveriam integrar o produto para fazer a referida prova".

129 João Calvão da Silva - *Responsabilidade Civil do Produtor*. ed. Coimbra: Livraria Almedina, 1999. ISBN: 972-40-0477-5. p. 470. Nesse mesmo sentido cfr. Juliana Campos - "A responsabilidade civil do produtor pelos danos causados por rôbos inteligentes à luz do regime do Decreto-Lei n.º 383/89, de 6 de novembro". *Revista de Direito da Responsabilidade* cit. p. 710.

130 Cf. Acórdão da Relação do Porto de 13/07/2000, Processo n.º 0030835, Relator Moreira Alves, disponível em www.dgsi.pt.

nível no mercado, dá lugar à responsabilidade objetiva do produtor. Contudo, para a mobilização deste regime, exige-se a observância de quatro requisitos, a saber: o produtor, o produto, o defeito e o momento da entrada em circulação do produto no mercado[131]. Vejamos.

i. O produtor

Desde logo, exige-se a presença de um produtor (art. 2.º). O conceito de produtor deve ser entendido *in lato sensu*, tal como entendeu o legislador comunitário na Diretiva 85/374/CEE, de 25 de julho de 1985. Desta forma, amplia-se a proteção do consumidor-lesado, tornando mais fácil a atribuição de culpa ao obrigado, no seio da complexa cadeia distributiva. Assim, incorporamos no conceito de produtor, o produtor real ou efetivo[132] (1ª parte do n.º 2 do art. 2.º), o produtor aparente[133] (2ª parte do n.º 2 do art. 2.º) e o produtor presumido[134], quer seja comunitário ou produtor absolutamente presumido (al. a) do n.º 2 do art. 2.º), quer seja o fornecedor de produto anónimo ou produto relativamente presumido (al. b) do n.º 2 do art. 2.º).

Nestes termos, verifica-se que o conceito de produtor de dispositivos inteligentes engloba, entre outros, os fornecedores de sensores, o programador informático, o produtor do *software*, o vendedor, etc. Note-se que o conceito de produtor é variável. Ele ajustar-se-á conforme o setor comercial a que pertence o dispositivo inteligente. Exemplificando, no caso de um brinquedo inteligente, além dos obrigados citados acima, farão também parte

---

131 Juliana Campos - "A responsabilidade civil do produtor pelos danos causados por rôbos inteligentes à luz do regime do Decreto-Lei n.º 383/89, de 6 de novembro". *Revista de Direito da Responsabilidade* cit. p. 708. "Para a mobilização do regime da responsabilidade objetiva do produtor, exige-se a observância de quatro requisitos: o produtor, o produto, o defeito e o momento da entrada em circulação"

132 Entendemos como produtor real ou efetivo "qualquer pessoa humana ou jurídica que sob a sua própria responsabilidade participa na criação do produto final, sejam o fabricante do produto acabado, de uma parte componente ou de matéria-prima". João Calvão da Silva - *Responsabilidade Civil do Produtor*, cit., p. 546. Nesse sentido, cfr. Vera Lúcia Paiva Coelho - Responsabilidade do produtor por produtos defeituosos "Teste de resistência" ao DL n.º 383/89, de 6 de novembro, à luz da jurisprudência recente, 25 anos volvidos sobre a sua entrada em vigor. *Revista Eletrónica de Direito* cit. p. 10.

133 Por sua vez, o produtor aparente acaba por ser o distribuidor, o grossista ou as grandes cadeias comerciais, apesar de não ser o fabricante do produto acabado ou final, coloca no mesmo a sua marca ou símbolo distintivo, induzindo o lesado em erro, quanto à origem ou proveniências de fabricação do produto, dando-lhe a aparência de ser ele próprio o produtor real. (Cfr. Maria Afonso e Manuel Variz - *Da Responsabilidade Civil Decorrente de Produtos Defeituosos*. ed. Coimbra: Coimbra Editora, 1991. ISBN: 972-32-0466-5. p. 27.)

134 Nestes termos o importador e fornecedor não são produtores propriamente ditos, mas são apelidados de produtores, respondendo, nos mesmos termos que o produtor real ou aparente. Fernando Simões Dias, *Marca do distribuidor e responsabilidade por produtos*, p. 93. (Nesse sentido, cfr. Vera Lúcia Paiva Coelho - Responsabilidade do produtor por produtos defeituosos "Teste de resistência" ao DL n.º 383/89, de 6 de novembro, à luz da jurisprudência recente, 25 anos volvidos sobre a sua entrada em vigor. *Revista Eletrónica de Direito* cit. p. 12.)

do conceito os sujeitos incluídos na expressão "operadores económicos", conforme o art. 3.º do Decreto-Lei n.º 43/2011, de 24 de março, que estabelece as regras de segurança dos brinquedos disponibilizado no mercado; i.e., o fabricante, o mandatário, o importador e o distribuidor.

ii. O produto

No que se refere ao requisito do produto, deve-se atender ao n.º 1 do art. 3.º, o qual estabelece que produto é "qualquer coisa móvel, ainda que incorporada noutra coisa móvel ou imóvel", pelo que o critério decisivo, aqui, é a incorporação, e não a destinação ou finalidade desse bem[135]. Posto isto, precisamos de averiguar se as tecnologias pertencentes à IdC respondem a tal definição. Vejamos.

Em primeiro lugar, o conceito de produto inteligente tem de corresponder ao conceito de *res* para corresponder ao conceito de produto definido no n. º1 do art. 3.º. A noção de "coisa" está consagrada no n.º 1 do art. 202.º do CC: "Diz-se coisa tudo aquilo que pode ser objeto de relações jurídicas". Entre nós, consideramos que é uma noção imprecisa e inadequada, pelo que acompanhamos a posição de Mota Pinto que densifica o preceito. Por um lado, ele considera "coisas" — em sentido jurídico — "bens (ou entes) de carácter estático, desprovidos de personalidade e não integradores do conceito necessário desta, suscetíveis de constituírem objeto de relações jurídicas". Por outro lado, o autor explica que para uma *res* ser considerada objeto de relações jurídicas, ela tem de reunir os seguintes traços: a existência autónoma e separada, possibilidade de apropriação exclusiva por alguém, aptidão para satisfazer necessidades humanas[136]. Assim "cabem, neste conceito, todos os tipos de bens produzidos, independentemente de se tratar de bens de consumo, como eletrodomésticos, brinquedos ou bens de produção"[137]. Posto isto, os dispositivos inteligentes parecem satisfazer os traços invocados, e, por conseguinte, correspondem ao conceito de "coisas" consagrado no n.º 1 do art. 202º.

Em segundo lugar, o dispositivo inteligente tem de ser uma coisa móvel. Aplicamos, para este efeito, o disposto no n.º 1.º do art. 205.º do CC: "São móveis todas as coisas não compreendidas no artigo anterior" (que refere as coisas imóveis). Assim sendo, concluímos que um relógio inteligente para crianças, uma boneca inteligente, um monitor de vídeo para bebés são exem-

---

135 Juliana Campos - "A responsabilidade civil do produtor pelos danos causados por rôbos inteligentes à luz do regime do Decreto-Lei n.º 383/89, de 6 de novembro". *Revista de Direito da Responsabilidade* cit. p. 709

136 carlos Alberto Da Mota Pinto; António J M Pinto Monteiro [et.al.] - Teoria geral do direito civil, cit., p. 343. "É que os bens de carácter estáticos, carecidos de personalidade, só são coisas em sentido jurídico quando puderem ser objetos de relações jurídicas. Para esse efeito devem apresentar as seguintes características: a) existência autónoma ou separadas...)

137 Acórdão da relação do Porto, de 14/10/2010 do Relator Henrique Antunes. Disponível em: www.dgsi.pt

plos de dispositivos inteligentes que encaixam na definição do mencionado artigo, e também no número 1.º do art. 3.º do Decreto-Lei n.º 383/89.

Note-se que, nos termos dos referidos artigos, ficam de fora da noção de produto, as coisas imóveis, i.e., os sistemas de irrigação inteligentes[138], postes de iluminação inteligentes, paneis fotovoltaicos em semáforos ou em sinais de trânsito[139], que são consideradas, enquanto produtos finais, *res* imóveis, e, portanto, não serão consideradas no âmbito normativo do n.º 1 do art. 3.º. Ressaltamos, no entanto, que devemos, em matéria de responsabilidade, averiguar a fonte que tornou o produto defeituoso, isto é o nexo do defeito com o dano. Nesta esteira, sabemos que uma coisa inteligente, é uma *res* complexa, composta por vários componentes. Ora, um poste de iluminação inteligente, mesmo sendo — enquanto produto final — uma coisa imóvel, ele funciona por meio de sensores, eletricidade, lâmpadas, etc. Sendo assim, se o defeito provir de um sensor, por exemplo, haverá então lugar à responsabilidade do produtor conforme o do n.º 1 do art. 3.º, pois é uma coisa móvel incorporada noutra coisa imóvel.

iii. O defeito

No que diz respeito ao conceito de produto defeituoso consagrado no n.º 1, do art. 4.º: "Um produto é defeituoso quando não oferece a segurança com que legitimamente se pode contar, tendo em atenção todas as circunstâncias, designadamente a sua apresentação, a utilização que dele razoavelmente possa ser feita e o momento da sua entrada em circulação."

Posto isto, concluímos que a noção de produto defeituoso "repousa na falta de segurança legitimamente esperada do produto e não na falta de conformidade ou qualidade, na aptidão ou idoneidade do produto para a realização do fim que se destina"[140]. Ou seja, um produto que apresente falha de segurança, é um produto defeituoso.

Esclarecemos, contudo, que não se exige uma segurança absoluta, mas sim uma "segurança com que legitimamente se possa contar". No fundo, de-

---

138 Leverege, *IoT 101 An Introduction to the Internet of Things* [Em linha]. First Edition, 2018. [Consult. 2021-02-22]. Disponível na Internet: < URL: https://indd.adobe.com/view/d38aec14-b884-492d-ba9f-de7ffe59ac6c>. p. 14. Os sistemas de irrigação inteligente "could be sensing soil moisture and taking weather into account so that smart irrigation systems only water crops when need, reducing the amount of water usage (…) allows monitoring and management of micro-climate conditions (humidity, temperature, light, etc.) to maximize production."

139 Iberdrola - *'Smart cities': a revolução tecnológica chega às cidades* [Em linha]. [Consult. 2021-08-23]. Disponível na Internet: <URL: https://www.iberdrola.com/inovacao/smart-cities>.

140 Acórdão do Supremo Tribunal de Justiça de 11/03/2003 do Relator Afonso Correia, disponível em www.dgsi.pt.

ve-se atender às "expectativas objetivas do público em geral"[141]. A avaliação da situação jurídica deve ser levada a cabo de uma forma objetiva, abstraindo a perspetiva de um determinado consumidor. Pelo contrário, devemos ter em conta, na determinação do carácter defeituoso, aquilo que o grande público consumidor pode legitimamente contar[142], mas sempre "tendo em atenção a peculiaridade do produto em causa e todas as circunstâncias do caso concreto" [143]. Fundamentalmente, a segurança esperada e tida por normal é avaliada pelas conceções do tráfico do respetivo setor de consumo[144].

Consequentemente, compreende-se que, aquando da colocação de um brinquedo inteligente no mercado, e.g., impõe-se que se tenha em conta o facto do brinquedo ser um produto concebido e destinado a ser utilizado por crianças. Assim sendo, o produtor deve considerar a vulnerabilidade[145] agravada do consumidor-criança. Contudo, relembramos que a dita debilidade é relativa, portanto, o grau de vulnerabilidade é medido em função da idade e do estado de desenvolvimento do menor. Esta relatividade irá influenciar a determinação de segurança do produto, i.e., se ele é de facto considerado defeituoso ou não. Como explica Mafalda Miranda Barbosa "um produto pode ser seguro e não o ser, se a categoria preferencial de consumidores a que se destina forem crianças ou os idosos[146]". As IdC para crianças devem ser produtos adaptados ao desenvolvimento e a capacidade do menor. Do

---

141 Juliana Campos - "A responsabilidade civil do produtor pelos danos causados por rôbos inteligentes à luz do regime do Decreto-Lei n.º 383/89, de 6 de novembro". *Revista de Direito da Responsabilidade.* cit. p. 710.

142 Maria Afonso [et.al.] - *Da Responsabilidade Civil Decorrente de Produtos Defeituosos*, cit., p. 27.

143 João Calvão da Silva - *Responsabilidade Civil do Produtor*, cit., p. 637. "... um produto não é defeituoso porque oferece um bom nível de segurança conforme às legítimas expectativas do público...".

João Calvão da Silva - *Responsabilidade Civil do Produtor*, cit., p. 636. "... deve atender, não às expectativas subjetivas dos lesado, à segurança com que ele pessoalmente contava, mas as expectativas objetivas do "público em geral", isto é, à segurança esperada e tida por normal nas conceções do tráfego do respetivo setor de consumo, v.g, de adultos, menores, de deficientes, etc.".

144 João Calvão da Silva - *Responsabilidade Civil do Produtor*, cit., p. 635. "A lei não exige que o produto ofereça uma segurança absoluta, mas apenas a segurança com que se possa legitimamente contar."

145 Neste sentido, *vide* Acórdão do Tribunal de Justiça de 5/03/2015, Processo C-503/13 e C-504/13, no qual considerou que "Quanto a dispositivos médicos, como os estimuladores cardíacos e os desfibrilhadores implantáveis em causa nos processos principais, há que referir que, tendo em conta a sua função e a situação de particular vulnerabilidade dos pacientes que utilizam os referidos dispositivos, as exigências de segurança que esses pacientes podem legitimamente esperar dos mesmos são particularmente elevadas [...]" Disponível em: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=162686&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=161892> [consultado 23 de agosto de 2021]. [consultado 23 de agosto de 2021].

146 Mafalda Miranda Barbosa - Obrigação geral de segurança e responsabilidade civil. *Estudos de Direito do Consumidor.* cit. p. 290.

mesmo modo, o produtor deve sempre adotar condições e medidas de segurança reforçadas para acautelar a esfera jurídica do menor, assim como respeitar as disposições normativas do setor[147] em causa e satisfazer sempre o interesse superior da criança. Neste sentido, a Comissão Europeia, na elaboração da Nova Agenda do Consumidor[148] reconheceu a vulnerabilidade da criança enquanto utilizadora de objetos conectados, e por isso, no seu plano de Ação 17 definiu que "Em 2021, a Comissão prevê preparar uma decisão sobre requisitos de segurança a cumprir pelas normas relativas aos produtores para crianças, para além de reforçar o quadro de segurança dos produtos através de uma proposta de revisão da Diretiva Segurança Geral dos Produtos".

Adicionalmente, o n.º 1, do art. 4.º do decreto-lei refere "...tendo em atenção todas as circunstâncias, designadamente a sua apresentação...", apontando no sentido de que o produtor deve considerar adaptar a sua abordagem em função do seu potencial consumidor. Assim, as condições de utilização, por exemplo, devem ser explicitas, isto é, devem apresentar-se de modo adaptado, com linguagem clara e fácil para os menores, como também para aqueles que têm funções de cuidado e que lidam com eles[149].

Ademais, ter-se-á em consideração o nível da ciência e das técnicas empregues no âmbito das tecnologias da informação e da comunicação, ao tempo em que o dispositivo inteligente foi posto no mercado. Esta imposição normativa faz recair sobre o produtor a obrigação de estar sempre a par do mais avançado estado da ciência e da técnica mundiais, tendo de provar cabalmente que não podia prever, nem evitar a concretização dos danos por falta ou insuficiência dos conhecimentos técnicos e científicos na data do lançamento do produto no mercado[150].

Por mais, outro ponto de destaque é o sistema operativo das IdC que pode ser um *software* (geralmente) ou um *hardware.* Relativamente a este as-

---

147 Relativamente a segurança dos brinquedos inteligente deverá respeitar as disposições do Decreto-Lei n.º 43/2011, que transpõe a Diretiva n.º 2009/48/CE, e, paralelamente, outros documentos legislativos, como o Regulamento Geral da Proteção de Dados, a Lei da Defesa dos Consumidores, o Decreto-Lei relativo a venda de bens de consumo e das garantias a ELA relativas, etc.

148 COM(2020) 696 final - *Nova Agenda do Consumidor - Reforçar a resiliência para uma recuperação sustentável* Bruxelas 2020b.

149 L'enfant, Comité des droits de - *Observation générale n.º25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique* 2021. Disponível na Internet: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2f5F0vEG%2bcAAx34gC78FwvnmZXGFsdFXGQsWU46nx%2b5vAg3QbGXlnOwo3Oquj 2b5vAg3QbGXlnOwo3Oquj8nN7ltX6yUYoRpe7N%2b7Q6mEUlz2mfWi>. p. 5. No âmbito das medidas legislativas, administrativa e outras a serem tomadas "Ils devraient également répondre aux besoins des enfants défavorisés ou vulnérables, notamment en fournissant des informations qui soient adaptées aux enfants et, si nécessaire, traduites dans les langues minoritaires pertinente".

150 Vera Lúcia Paiva Coelho - Responsabilidade do produtor por produtos defeituosos "Teste de resistência" ao DL n.º 383/89, de 6 de novembro, à luz da jurisprudência recente, 25 anos volvidos sobre a sua entrada em vigor. *Revista Eletrónica de Direito* cit. p. 43.

sunto, a União Europeia determina que o fabricante do produto final tem a obrigação de — no âmbito da avaliação inicial dos riscos — prever os riscos associados ao sistema operativo, no momento da sua colocação no mercado. Além do mais, a UE reconhece que há riscos decorrentes de posteriores atualizações dos mesmos. Neste aspeto, a CE compara as atualizações com as operações de manutenção por motivos de segurança desde que não alterem significativamente o produto colocado no mercado e nem introduzam novos riscos não previstos na avaliação inicial dos riscos, porque, se isto acontecer, o produto será tido como um novo produto, devendo a sua conformidade — em matéria de segurança dos produtos — ser reavaliada[151].

Complementarmente, no que diz respeito aos *software* autónomos"[152], a Comissão Europeia reconhece que poderá ser necessário incluir requisitos específicos e/ou explícitos relativos a estes nos diplomas normativos vigentes, no sentido de impor obrigações adicionais aos fabricantes para que estes incluam funcionalidades capazes de prevenir que o posterior carregamento de *software* autónomos, não comprometam a segurança do produto, ao longo da sua vida útil.

Ainda no campo do *software*, assumirá particular relevo saber quem tem o encargo de atualizar o dispositivo: se é o produtor, o utilizador, ou o proprietário. No nosso entendimento, o produtor tem o dever de informar o proprietário das atualizações necessárias e disponíveis. Depois de comunicado, se a atualização não é efetuada, e, por conta disso ocorrer um dano, haverá culpa do lesado, podendo ser a responsabilidade do produtor excluída (n.º 1, art. 7.º)[153].

Resumidamente, o conceito de produto defeituoso é um termo muito abrangente, que é alargado face às tecnologias pertencentes à IdC. De facto, tal como vimos, perante os dispositivos inteligentes, deve-se atender à coexistência de defeitos provenientes da sua capacidade de conectividade, da complexidade do seu sistema e da cadeia de produção, do desenvolvimento da ciência aquando da sua entrada no tráfego, às suas atualizações de sistemas operativos, entre outros que se mostrarem pertinentes na avaliação do defeito.

iv. O momento da entrada em circulação

Por último, segundo Cassiano dos Santos, o quarto requisito referente ao momento da colocação do produto no mercado, significa "a saída de produ-

---

151 COM(2020) 64 final - *Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica*. Bruxelas: 2020a.

152 O *software* autónomo é aquele que pode ser colocado separadamente no mercado ou carregado para um produto após a colocação deste no mercado.

153 Juliana Campos - "A responsabilidade civil do produtor pelos danos causados por rôbos inteligentes à luz do regime do Decreto-Lei n.º 383/89, de 6 de novembro". *Revista de Direito da Responsabilidade* cit. p. 710.

to da esfera de produção e a sua entrada no circuito de distribuição"[154], ou seja, corresponde ao momento em que o produtor lança livre e voluntariamente o produto no mercado ou na cadeia económica de distribuição[155].

b) A responsabilidade relativa do produtor

A responsabilidade objetiva do produtor é relativa. De facto, a responsabilidade decorrente de produtos defeituosos é uma responsabilidade objetiva que requer a verificação de um nexo de ligação entre o defeito do produto e os danos sobrevenientes[156]. Ou seja, caso se verifique uma das situações previstas no art. 5.º, haverá exoneração da responsabilidade ao lesante, que levará à extinção da obrigação do produtor de reparar o dano[157].

Como já referimos, na situação hipotética de um brinquedo inteligente não ser atualizado por culpa do progenitor do menor em causa, e se se verificar alguma falha de segurança derivada da falta de atualização do *software,* que por sinal, bloqueava ou reparava tal defeito, haverá exoneração do produtor, respondendo pelos danos causados o proprietário do produto.

c) A responsabilidade solidária

Em conformidade com o art. 6.º, a responsabilidade do produtor é uma responsabilidade solidária, ou seja, todos aqueles que intervêm na cadeia de produção — desde a concessão até o fim da vida útil do produto — são responsáveis pelo produto defeituoso e, por conseguinte, podem ser solidariamente demandados pelo lesado, pois eles são solidariamente responsáveis pelo dano ocorrido[158].

---

154 Filipe Cassiano dos Santos - *Direito Comercial Português* 1ª ed. Coimbra 2007. ISBN: 9789723214956. p. 207. Nesse mesmo sentido cfr. BARBOSA, Mafalda Miranda - Obrigação geral de segurança e responsabilidade civil. *Estudos de Direito do Consumidor.* cit. p. 288.

155 João Calvão da Silva, "Responsabilidade civil do produtor" p.637. No mesmo sentido, cfr. CAMPOS, Juliana – "A responsabilidade Civil do produtor pelos danos causados por robôs inteligentes...", p. 710.

156 Mafalda Miranda Barbosa - Obrigação geral de segurança e responsabilidade civil. *Estudos de Direito do Consumidor.* cit. p. 332.

157 Vera Lúcia Paiva Coelho - Responsabilidade do produtor por produtos defeituosos "Teste de resistência" ao DL n.º 383/89, de 6 de novembro, à luz da jurisprudência recente, 25 anos volvidos sobre a sua entrada em vigor. *Revista Eletrónica de Direito* cit. p. 29. "Considera a Diretiva que estas causas de exoneração tornam a relação comercial mais justa, por existir uma equitativa repartição dos riscos entre produtor e lesado...".

158 Vera Lúcia Paiva Coelho - Responsabilidade do produtor por produtos defeituosos "Teste de resistência" ao DL n.º 383/89, de 6 de novembro, à luz da jurisprudência recente, 25 anos volvidos sobre a sua entrada em vigor. *Revista Eletrónica de Direito* cit. p. 31. "O dano que se consubstancia no prejuízo propriamente dito sofrido pelo consumidor, em virtude de um produto defeituoso, é um dos pressupostos constitutivos da responsabilidade objetiva a ser objeto de prova, por parte do lesado, de forma a haver responsabilização do produtor. Desta forma, para que essa responsabilidade se constitua plenamente, o lesado terá de alegar e provar que o dano existe e que decorreu de um defeito presente num produto"

Note-se que, caso o lesado seja uma criança, ela deve ser representada em juízo. Na verdade, embora o menor, nos termos do art. 11.º do Código de Processo Civil (CPC), seja titular de personalidade judiciária, ele não tem capacidade jurídica (art. 123.º do CC e art.15.º do CPC) e, portanto, não pode estar, por si só, em juízo. O suprimento da sua incapacidade é feito através do instituto da representação legal, por viés da representação parental (art.º 124.º e art.º 1878.º do CC), ou da tutela (art. 124.º e 1921.º do CC), e, se for caso, através de um curador provisório (n.º 1 do art. 17.º do CPC).

5.3. VIOLAÇÃO DA OBRIGAÇÃO GERAL DE SEGURANÇA

Um produto defeituoso é, como vimos *supra,* um produto que apresenta falhas de segurança e, por conseguinte, é uma fonte de riscos para os seus utilizadores. O nosso ordenamento jurídico reconhece a vulnerabilidade do consumidor na relação de consumo, e, por isso, envida esforços destinados a assegurar uma proteção eficiente e adequada ao consumidor. Como resultado, há uma obrigação geral de segurança, que como o próprio nome indica, diz respeito à segurança de todos os produtos postos em circulação. Esta obrigação diz-se geral, quer porque ela vincula todos os produtores, quer porque se apresenta como não setorial[159].

Entre nós, a obrigação geral de segurança está consagrada no Decreto-Lei n.º 69/2005, de 17 de março, que transpõe para a ordem jurídica interna a Diretiva n.º 2001/95/CE, do Parlamento Europeu e do Conselho, de 3 de dezembro, relativa à segurança geral dos produtos.

A violação da obrigação geral de segurança ocorrerá com a colocação de um produto no tráfego, que não cumpre os requisitos de segurança, i.e., de um produto defeituoso. Tal situação determina a responsabilidade objetiva dos obrigados, a qual dá lugar a uma responsabilidade contraordenacional, nos termos da al. e), n.º 1 do art. 26.º do Decreto-Lei n.º 69/2005, e pode ainda desencadear uma pretensão indemnizatória fundada em responsabilidade civil, nos termos do artigo 483.º do CC[160].

5.4. CONSIDERAÇÕES FINAIS

Verificamos que o Decreto-Lei n.º 383/89, apesar da sua neutralidade relativamente às novas tecnologias e às lacunas supervenientes associadas a este meio, ainda assim, consegue e deve ser aplicado face às vicissitudes oriundas do ambiente conectado para proteger as vítimas de danos provocados por dispositivos inteligentes defeituosos. Para tal, exige-se a

---

159 Mafalda Miranda Barbosa - Obrigação geral de segurança e responsabilidade civil. *Estudos de Direito do Consumidor.* cit. p. 274. "A obrigação diz-se, assim, geral quer porque vincula todos os produtores, quer porque se apresenta como não setorial".

160 Mafalda Miranda Barbosa - Obrigação geral de segurança e responsabilidade civil. *Estudos de Direito do Consumidor.* cit. p. 294-295.

observância de quatro requisitos para a mobilização do regime. O primeiro requisito refere-se ao produtor, que é um conceito variável conforme o setor comercial a que ele pertence e deve ser entendido em *lato sensu,* abarcando todos os intervenientes na cadeia de produção, distribuição e de manutenção do dispositivo inteligente. Em segundo lugar, temos o requisito produto, que determina que os dispositivos inteligentes devem ser coisas móveis, nos termos gerais do n.º 1, do art. 202º do CC. O terceiro requisito é o defeito. Ele repousa na falta de segurança que legitimamente pode se esperar do produto, principalmente, quando este foi concebido e destinado para ser utilizado por crianças. Neste caso, o produtor deve considerar a vulnerabilidade agravada do consumidor-criança, adotando deste modo, medidas de segurança reforçadas para acautelar a esfera jurídica dos mais novos, com vista a satisfazer o seu interesse superior. E por último, o quarto requisito, que diz respeito ao momento da entrada em circulação do produto no mercado que corresponde ao instante em que o produtor lança livre e voluntariamente o produto no mercado.

Todavia, as emergências dos produtos inteligentes e seu previsível crescimento, colocam novos desafios em termos de segurança dos produtos e da responsabilidade. Tal como vimos, eles advêm de diferentes fontes, entre elas, por exemplo, a conectividade, a complexidade dos seus produtos, inclusive, a sua própria estrutura física, as atualizações de *software.*

Deste modo, a fim de corrigir as incertezas e eliminar as suas atreladas dificuldades em matéria de responsabilidade, reclama-se a necessidade do referido decreto-lei (assim como outras legislações gerais e setoriais no âmbito do direito do consumo) ser revisto e atualizado, de modo a assegurar a posição do consumidor. Em particular, apela-se que seja tida em consideração a especial posição do consumidor-criança, que, representando, a geração de utilizadores mais envolvidos neste ambiente, e aqueles que, atualmente, são os mais lesados por dispositivos com falhas de segurança, merecem medidas especiais, que sejam pensadas no seu superior interesse e que visem protegê-los de modo adequado e eficaz.

6. CONCLUSÃO

O atual e célere progresso tecnológico transforma e impacta consideravelmente as vidas dos mais novos, que, pela sua notável utilização de produtos pertencentes à Internet das Coisas, apresentam-se, no tráfego jurídico, como verdadeiros consumidores. No entanto, devido à sua especial situação de menoridade, os infantes sofrem de uma vulnerabilidade agravada, e por isso, merecem uma proteção especial de acordo com o seu grau de fragilidade, que ao longo dos anos se dilui, até atingir a maioridade.

Complementarmente, os produtos da IdC, ao mesmo tempo que oferecem novas oportunidades, eles tendem — frequentemente — a lesar os direitos das crianças, pois, facilmente, expõem os menores a situações de perigos provenientes de falhas de segurança do produto inteligente. Tais anomalias originam-se em diferentes fontes, entre muitas, destacam-se a capacidade de conectividade; o grau de complexidade dos aparelhos inteligentes, que combinam diferentes produtos e chamam vários agentes para a sua elaboração, produção e manutenção, o que dificulta a determinação da origem do problema e por conseguinte, a atribuição da responsabilidade. Além do mais, os atuais diplomas em matéria de proteção e segurança do produto foram elaborados antes da emergência da Internet das Coisas, e, portanto, é preciso estabelecer requisitos de segurança atualizados, em especial, para os produtos destinados às crianças, além de adaptar o regime normativo vigente em matéria de segurança do produto e responsabilidade do produtor.

O mundo conectado é uma realidade do dia-a-dia das crianças com tendência a crescer cada vez mais. Perante este facto, o Direito necessita reunir esforços para garantir que os direitos dos menores sejam assegurados no mundo digital. Para tal, é preciso adaptar os diplomas normativos vigentes de modo que estes façam referência direta aos novos desafios que o ambiente conectado traz e, deste modo, zelar pela promoção e proteção dos direitos dos menores em todas as situações, sejam elas advindas do mundo físico ou do mundo *online*, tendo em conta que vivemos hoje, nas palavras do jurista italiano Rodotà, numa "mixed reality[161]".

7. REFERÊNCIAS BIBLIOGRÁFICAS

Afonso, Maria; Variz, Manuel - *Da Responsabilidade Civil Decorrente de Produtos Defeituosos*. ed. Coimbra: Coimbra Editora, 1991. ISBN: 972-32-0466-5.

Barbosa, Mafalda Miranda - Obrigação geral de segurança e responsabilidade civil. *Estudos de Direito do Consumidor*. Coimbra Faculdade de Direito Universidade de Coimbra [Em linha]. Vol: 14 (2018) p. 273-341. ISSN: 1646-0375.

Batat, Wided - Comment les adolescents définissent-ils leurs propres compétences en matière de consommation ? Une approche par les portraits - *Recherche et Applications en Marketing (French Edition)* [Em linha]. Vol: 29, nº 1 (2014), p. 27-60. Disponível na Internet: <https://journals.sagepub.com/doi/abs/10.1177/0767370113505946>.

Brander, Patrícia [Et Al.] - *Compass* [Em linha]. 1ª ed. Guide - Artes Gráficas, Lda., 2016. [Consult. 2021-04-19]. Disponível na Internet: <URL: https://www.dge.mec.pt/compass-manual-de-educacao-para-os-direitos-humanos-com-jovens>. ISBN 978-989-99443-1-2.

161 *Vide* nota 25.

Bernardino, Carla – "2020 sentou mais 350 mil portugueses por dia em frente à TV. A maioria a pagar [Em linha]". *Diário de Notícias*. [Consult. 2021-09-14]. Disponível na Internet: <URL: https://www.dn.pt/edicao-do-dia/03-jan-2021/2020-sentou-mais-350-mil-portugueses-por-dia-em-frente-a-tv-a-maioria-a-pagar-13188007.html>.

Brito, Rita; Dias, Patrícia; Oliveira, Gabriela – "Young Children, Digital Media and Smart Toys: How Perceptions Shape Adoption and Domestication" - *British Journal of Educational Technology* [Em linha]. Vol: 49, nº 5 (2018), p. 807-820. [Consult. 2020-04-30]. Disponível na Internet: <http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1190597&site=eds-live>. ISSN: 0007-1013

Campos, Juliana - A responsabilidade civil do produtor pelos danos causados por rôbos inteligentes à luz do regime do Decreto-Lei n.º 383/89, de 6 de novembro. *Revista de Direito da Responsabilidade* [Em linha]. Vol: ANO 1 (2019) p. 700-730. [Consult. 2021-08-21]. Disponível na Internet: <URL: https://revista-direitoresponsabilidade.pt/2019/a-responsabilidade-civil-do-produtor-pelos-danos-causados-por-robos-inteligentes-a-luz-do-regime-do-decreto-lei-n-o383-89-de-6-de-novembro-juliana-campos/>. ISSN: 2184-4542.

canotilho, josé joaquim gomes - *Direito constitucional e teoria da constituição*. 7ª ed. Coimbra: Almedina, 2018. ISBN: 978-972-40-2106-5.

Canotilho, José Joaquim Gomes; Moreira, Vital - *Constituição da República Portuguesa anotada*. 4ª rev. ed. Coimbra: Coimbra Editora, 2007. ISBN: 972-32-1462-8.

Carvalho, Diógenes Faria De; Oliveira, Thaynara De Souza – "A categoria jurídica de 'consumidor-criança' e sua hipervulnerabilidade no mercado de consumo brasileiro". *Revista Luso-Brasileira de Direito do Consumo* [Em linha]. Vol: V N.º 17 (2015) p. 207-230. [Consult. 2020-03-20]. Disponível na Internet: <URL: https://app.vlex.com/#vid/561354770>.

Carvalho, Jorge Morais - *Manual de Direito do Consumo* 1ªed. 2013. ISBN: 978-972-40-5377-6.

Carvalho, Orlando De - *Teoria geral do direito civil*, 3ªed. Coimbra: Coimbra Editora 2012. ISBN:978-972-32-2017-9.

Castells, Manuel - *A sociedade em rede*. 8ª Revista e Ampliada ed. São Paulo: Paz e terra 2005

Coelho, Vera Lúcia Paiva - Responsabilidade do produtor por produtos defeituosos "Teste de resistência" ao DL n.º 383/89, de 6 de novembro, à luz da jurisprudência recente, 25 anos volvidos sobre a sua entrada em vigor. *Revista Eletrónica de Direito*, Porto Faculdade de Direito Universidade do Porto [Em linha]. Vol: N.º 2 (2017) p. 1-54. Disponível na Internet: <URL: https://cije.up.pt/pt/red/edicoes-anteriores/2017-nordm-2/responsabilidade-do-produtor-por-produtos-defeituosos-ldquoteste-de-resistenciardquo-ao-dl-nordm-38389-de-6-de-novembro-a-luz-da-jurisprudencia-recente-25-anos-volvidos-sobre-a-sua-entrada-em-vigor/>. ISSN: 2182-9845.

commission, european - *Alert number: A12/0157/19* [Em linha]. Germany: European Commission. [Consult. 2021-08-06]. Disponível na Internet: <URL: https://ec.europa.eu/safety-gate-alerts/screen/webReport/alertDetail/349994>.

consommateurs, option - *Enfants sous écoute La protection de la vie privée dans l'environnement des jouets intelligents* 2018. [Consult. 2020-04-22]. Disponível na Internet: <URL: www.option-consommateurs.org>.

droits, défenseur des - Monde Numérique: Quels Droits? In DROITS, DÉFENSEUR DES - *Educadroit - Manuel d'éducation au Droit* [Em linha]. Défenseur des droits, [Consult. 2021-03-02]. p. 17. Disponível na Internet: <URL: https://educadroit.fr/sites/default/files/Manuel-Education-au-Droit-2020-chap11.pdf>.

económica, autoridade de segurança alimentar e - *RAPEX (Rapid Alert System for all dangerous consumer Products)* [Em linha]. [Consult. 2021-08-21]. Disponível na Internet: <URL: https://www.asae.gov.pt/inspecao-fiscalizacao/sistemas-de-alerta-e-troca-de-informacao/rapex.aspx>.

falcão, david - *Lições de Direito do Consumo* [Em linha]. 2ª Edição ed. Coimbra: Almedina, 2020. [Consult. 2021-09-07]. Disponível na Internet: <URL: https://ebooks.almedina.net/reader/books/9789724094168>.ISBN 978-972-40-9416-8.

flausch, manon - *Rapex, le système européen garant de la sécurité des produits* [Em linha]. EURACTIV.fr. [Consult. 2021-08-06]. Disponível na Internet: <URL: https://www.euractiv.fr/section/soci-t/news/rapex-le-systeme-europeen-garant--de-la-securite-des-produits/?_ga=2.113835584.679216804.1628262614-947037014.1628262614>.

gil, isabel cunha - Sinfonia do Supremo interesse da criança. *Boletim da Ordem dos Advogados*. Ordem dos Advogados. [Em linha]. (2019) [Consult. 2021-07-29]. Disponível na Internet: <URL: https://boletim.oa.pt>.

holloway, donell; green, lelia - The Internet of toys - *Communication Research & Practice* [Em linha]. Vol: 2, nº 4 (2016), p. 506-506-519. [Consult. 2020-04-14]. Disponível na Internet: <http://search.ebscohost.com/login.aspx?direct=true&-db=edb&AN=123147016&site=eds-live>. ISSN: 2204-1451

Horster, Heinrich Ewald - *A parte Geral do Código Civil Português - Teoria Geral do Direito Civil* 2ªed. Coimbra: Almedina, 2019. ISBN: 978-972-40-8146-5.

Iberdrola - *'Smart cities': a revolução tecnológica chega às cidades* [Em linha]. [Consult. 2021-08-23]. Disponível na Internet: <URL: https://www.iberdrola.com/inovacao/smart-cities>.

L'enfant, Comité Des Droits De - *Observation générale n.º25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique* 2021. Disponível na Internet: <URL: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2f5F0vEG%2bcAAx34gC78FwvnmZXGFsdFXGQsWU46nx%2b5vAg3QbGXlnOwo3Oquj8nN7ltX6yUYoRpe7N%2b7Q6mEUIz2mfWi>.

Leandro, Armando – "Promoção e Proteção dos Direitos da Criança". *Boletim da Ordem dos Advogados*. Ordem dos Advogados. [Em linha]. (2019) [Consult. 2021-07-29]. Disponível na Internet: <URL: https://boletim.oa.pt>.

Leverege, *IoT 101 An Introduction to the Internet of Things* [Em linha]. First Edition, 2018. [Consult. 2021-02-22]. Disponível na Internet: < URL: https://indd.adobe.com/view/d38aec14-b884-492d-ba9f-de7ffe59ac6c>.

Magrani, Eduardo - "Tudo o que é conectado é vulnerável". *Internet das coisas e inovação* [Em linha]. [Consult. 2020-11-23]. Disponível na Internet: <URL: http://eduardomagrani.com/tudo-que-e-conectado-e-vulneravel-diz-pesquisador/>.

— *Entre dados e robôs: ética e privacidade na era da hiperconectividade*. ed. Porto Alegre, RS: Arquipélago Editorial, 2019. ISBN: 9788554500290.

Magriço, Manuel – "A Internet e as crianças - riscos e potencialidades". In *JUDICIÁRIOS, CENTRO DE ESTUDOS - Coleção formação contínua: jurisdição da família e das crianças* [Em linha]. Lisboa: 2018. [Consult. 2021-08-03]. p. 9-32. Disponível na Internet: <URL: http://www.cej.mj.pt/cej/recursos/ebooks/familia/eb_InternetCriancas2018.pdf>. ISBN: 978-972-9122-98-9.

Martins, Rosa - *Menoridade, (in)capacidade e cuidado paternal*. 1ª ed. Coimbra: Coimbra Editora, 2008. ISBN: 978-972-32-1591-5.

Meira, Silvio - Sinais do futuro imediato, #1: internet das coisas. dia a dia, bit a bit [Em linha]. [Consult. 2021-03-13]. Disponível na Internet: <URL: https://silvio.meira.com/silvio/sinais-do-futuro-imediato-1-internet-das-coisas/>.

Mendes, João De Castro - *Direito civil: teoria geral* 2ª ed. ed. 1978.

Motti, Vivian Genaro – "Wearable Technologies: a Roadmap to the Future". *WebMedia'20: Proceedings of the Brazilian Symposium on Multimedia and the Web*. [Em linha]. (2020) p. 3-4. [Consult. 2021-03-19]. Disponível na Internet: <URL: https://dl.acm.org/doi/pdf/10.1145/3428658.3431928>. ISSN: 978-1-4503-8196-3.

Peppet, Scott R. – "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent" - *Texas Law Rewiew* [Em linha]. Vol: 93:85, nº (2014), p. 78. Disponível na Internet: <https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf>.

Pereira, Sara – "Os direitos da criança no mundo digital". *Forum de proteção de dados*. Lisboa: Comissão Nacional de Protecção de Dados. [Em linha]. Vol: [6 vol.] (2019) p. 8-17. Disponível na ISSN: 2183-5977.

Pinto, Carlos Alberto Da Mota; Monteiro, António J M Pinto; Pinto, Paulo Mota - *Teoria geral do direito civil*. 5ª ed. Coimbra: Gestlegal, 2020. ISBN: 978-989-8951-53-3.

Pita, Marina - Brinquedos conectados e os riscos à infância. Politics. Instituto Nupef. [Em linha]. (2019) p. 19-40. Disponível na Internet: <URL: https://politics.org.br/sites/default/files/downloads/nupef_politics29_web.pdf>. ISSN: 1984-8803.

Ponte, Cristina [Et Al.] - *Estudo crescendo entre ecrãs - Usos de meios eletrónicos por crianças (3-8 anos).* 2017. [Consult. 2021-02-22]. Disponível na Internet: <URL: https://www.erc.pt/documentos/Crescendoentreecras/mobile/index.html#p=1>.

Redinha, Maria Regina; Guimarães, Maria Raquel – "O uso do correio eletrónico no local de trabalho: algumas reflexões". In - *Estudos em homenagem ao Professor Doutor Jorge Ribeiro de Faria* [Em linha]. 2003. [Consult. 2021-08-24]. Disponível na Internet: <URL: https://repositorio-aberto.up.pt/handle/10216/24325>.

Rodotà, Stefano – *Palestra Professor Stefano Rodotà*. In Rio de Janeiro: 2003. [Consult. 2020-11-25]. Disponível na Internet: <URL: http://www.rio.rj.gov.br/dlstatic/10112/151613/DLFE-4314.pdf/GlobalizacaoeoDireito.pdf>. p. 1-11.

Santos, Filipe Cassiano Dos - *Direito Comercial Português* 1ª ed. Coimbra 2007. ISBN: 9789723214956.

Santos, Pedro Miguel Pereira - *Internet das coisas: O desafio da privacidade*. Setúbal: Instituto Politécnico de Setúbal 2016. 108 p. Tese de Mestrado.

Silva, João Calvão Da - *Responsabilidade Civil do Produtor*. 1ª ed. Coimbra: Livraria Almedina, 1999. ISBN: 972-40-0477-5.

Schor, Juliet B. - *Nascidos para comprar: uma leitura essencial para orientarmos nossas crianças na era do consumismo*. 1ª ed. São Paulo: Editora Gente, 2009. ISBN: 978-85-7312-570-2. p. 2.

Society, Internet - *C'est quoi un appareil de l'IdO?* [Em linha]. Internet Society. [Consult. 2021-02-22]. Disponível na Internet: <URL: https://www.internetsociety.org/fr/iot/>.

Telecomunicações, Grupo De Trabalho Internacional Sobre Proteção De Dados Nas - Dispositivos inteligentes para crianças e os riscos para a privacidade. *Forum de proteção de dados*. Lisboa: Comissão Nacional de Protecção de Dados. [Em linha]. Vol: [6 vol.] (2019) p. 38-49. Disponível na ISSN: 2183-5977.

— Proteção da privacidade das crianças nos serviços em linha. *Forum de proteção de dados*. Lisboa: Comissão Nacional de Protecção de Dados. [Em linha]. Vol: [6 vol.] (2019) Disponível na ISSN: 2183-5977.

Trajano Barbosa, Ohana ; Rodriguez Veloso, Andres – "Vulnerabilidade da Criança no Varejo: Um Estudo Sob a Perspectiva da Pesquisa Transformativa do Consumidor" - *GESTÃO.Org: Revista Eletrônica de Gestão Organizacional* [Em linha]. Vol: 15, nº 1 (2017), p. 1-1-10. [Consult. 2021-03-29]. Disponível na Internet: <https://periodicos.ufpe.br/revistas/gestaoorg/article/download/23042/24610>. ISSN: 1679-1827

Tomé, João - *Aparelho como a Smart TV crescem 12,3% em Portugal. Samsung lidera.* 2019. [Consut. 2021-08-05]. Disponível na Internet: <URL: https://insider.dn.pt/em-rede/aparelhos-como-a-smart-tv-crescem-123-em-portugal-samsung-lidera/19452/ >.

Vasconcelos, Pedro Pais De - *Teoria geral do direito civil* 6ª ed. ed. Coimbra 2010. ISBN: 978-972-40-4369-9.

Apresentação Smart Watch Infantil 4G, Wi-Fi e Bluetooth Relógio infantil GPS, Monitoramento Remoto. [Vídeo]. Realização de MOSTRAÊ! 2019. Disponível na Internet: <URL: https://www.youtube.com/watch?v=wBPYhKGTCLw>.

Nova Agenda do Consumidor - Reforçar a resiliência para uma recuperação sustentável COM(2020) 696 final Bruxelas 2020.

Reloj Inteligente para niños de Innjoo. [Vídeo]. Realização de WWWHATSNEW. 2020. Disponível na Internet: <URL: https://www.youtube.com/watch?v=iwXGo3yQp3Q>.

Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica. COM(2020) 64 final. Bruxelas: 2020.

Tab4you 6 é um Tablet Made in Portugal | Reportagem Futuro Hoje SIC. [Vídeo]. Realização de SCIENCE4YOU. 2019. Disponível na Internet: <URL: https://www.youtube.com/watch?v=Z7RF40PNVVI&t=22s>.

TechNews: Sistema operacional LG webOS une tecnologia e uma experiência completa - #JM. [Vídeo]. Realização de NEWS, Jovem Pan. 2021. Disponível na Internet: <URL: https://www.youtube.com/watch?v=KtHhriDH75c>.

ÍNDICE DE JURISPRUDÊNCIA

Supremo Tribunal de Justiça

Acórdão de 11/03/2003, Processo n.º 02A4341, do Relator Afonso Correia.

Tribunal da Relação do Porto

Acórdão de 11/09/2008, Processo n.º 0834643, do Relator Fernando Baptista.

Acórdão de 13/07/2000, Processo n.º 0030835, do Relator Moreira Alves

II

REGULAÇÃO DE DADOS PESSOAIS E PRIVACIDADE

THE IMPACT OF THE GENERAL DATA PROTECTION REGULATION (GDPR) ON ARTIFICIAL INTELLIGENCE

ARTICLE 22 THE RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION-MAKING

Antonia Karatza

up201909033@edu.direito.up.pt

Abstract: Artificial Intelligence, Machine-Learning algorithms, and Big Data are undoubtedly part of our lives. The purpose of the following analysis is to examine the tension between the EU General Data Protection Regulation (GDPR) provisions and Artificial Intelligence. We cover the main definition of Artificial Intelligence, Machine-Learning, and Big Data to better understand the way intelligent machines work. Moreover, we focus on the legal basis of Artificial Intelligence and the ethical challenges that arise from its use. We aim to analyze Article 22 of GDPR and the right not to be subjected to automated decision-making. The legal implications that arise from profiling are assessed while pointing out the risks but also the opportunities that Artificial Intelligence brings. To sum up, we will embrace the necessity of transparency, the existence of an ethical framework and the high importance of the Data Protection Impact Assessments for the protection of the data subjects' privacy rights. In this respect, this study analyses the legal provisions related to algorithms, while identifying the current challenges of the existence of a legal framework to Artificial Intelligence and the protection of personal data.

Keywords: GDPR; Artificial Intelligence; Big Data; automated decision-making; personal data; profiling; transparency.

Resumo: Inteligência Artificial, algoritmos de Machine-Learning, e Big Data são, sem dúvida, parte das nossas vidas. O objetivo desta análise é examinar a tensão entre as disposições do Regulamento Geral sobre a Proteção de Dados da UE (RGPD) e a Inteligência Artificial. Iremos aprofundar a principal definição de Inteligência Artificial, Machine-Learning, e Big Data para entender melhor a forma como as máquinas inteligentes funcionam. Além disso, concentramo-nos na base jurídica da inteligência artificial e dos desafios éticos decorrentes da sua utilização. Pretendemos analisar o Artigo 22.º do RGPD e o direito à não sujeição a decisões automatizadas. As implicações jurídicas decorrentes da definição de perfis são avaliadas ao mesmo tempo que indicamos os riscos, mas também as oportunidades que a Inteligência Artificial traz. Em suma, iremos defender a necessidade de transparência, a existência de um quadro ético e a elevada importância das avaliações de impacto da protecção de dados para a protecção dos direitos de privacidade dos titulares dos dados. A este respeito, este estudo analisa as disposições legais relacionadas com os algoritmos, identificando simultaneamente os atuais desafios da existência de um quadro jurídico para a Inteligência Artificial e a proteção de dados pessoais.

Palavras-chave: RGPD; Inteligência Artificial; Big Data; decisões automatizadas; proteção de dados; profiling; transparência.

1. INTRODUCTION

Artificial intelligence has been proven to be the biggest trigger for the so-called "fourth industrial revolution"[1], that is continuously changing the way our society functions and how humans relate to each other. The rise of intelligent machines, the appearance of Big Data and the invention of Machine-Learning methods constituted by complex algorithms, enabled the numerous decisions to be taken automatically, in every respect. There is no doubt that, at the moment, we are facing a range of legal issues in the search for a balance between considerable social advances in the name of AI regarding not only fundamental privacy rights but also personality rights in interpersonal relationships. The exponential increase in the use of the Internet, on the other hand, with the emergence of social networking, has introduced serious new challenges to the legal framework concerning privacy.

More than ever, from the moment we wake up until the moment we go to sleep, we use numerous online applications for banking services, financial services and online shopping, medical services, applications of public administration, all based on algorithms. Given the unproductiveness of adopting a fatalistic vision – "I've created a monster" –, it becomes necessary to know the difficulties triggered by the use of new technologies and understand their functioning, as we started by stating, and its potential, to better envisage the legal instruments provided by our civil law when faced with these realities.[2]

Several examples of AI, such as AI-supported voice-generating features in smartphones, virtual assistants[3] such as voice recognition models like Alexa or Siri, are capable of responding correctly to all types of user requests in the most diverse situations. Google Maps applications have saved us a lot of time as we do not put much thought into traveling to a new destination anymore. Autonomous vehicles are already becoming a reality and, anytime soon, they can be part of the street too.[4] Automated profiling, which enables companies to send targeted advertising to their consumers, such as Netflix

---

[1] Maja Brkan, *Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond*, International Journal of Law and Information Technology, January 2019, page 92, Available at: DOI; 10.1093/ijlit/eay017, (Last accessed: 05.09.2021).

[2] Maria Raquel Guimarães, *A tutela da pessoa e da sua personalidade: algumas questões relativas aos direitos à imagem, à reserva da vida privada e à reserva da pessoa íntima ou direito ao carácter*, *in A tutela geral e especial da personalidade humana — 2017* (Gabriela Cunha Rodrigues, Laurinda Gemas, Margarida Paz, orgs.), Lisboa, Centro de Estudos Judiciários, January 2018, page 35.

[3] European Parliament, "What is artificial intelligence and how is it used?", Article, European Parliament, 20200827STO85804, October 2020, Available at: https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used, (Last accessed: 06.09.2021).

[4] Bruno Fernando dos Santos Cruz, *Smart Cars: desafios jurídicos na era da inteligência artificial*, Master 's Thesis, Faculty of Law, University of Porto, December 2020.

that provides highly accurate predictive technology based on customer's reactions to films, is also a reality.

All these applications are made by dedicated AI solution-driven teams.[5] The new engineering science of AI is being held by companies like Microsoft, Amazon, Google, Facebook and IBM. Those are the main technological leaders, all located in the United States of America, that hold the power to decide and handle the usage of new methods and algorithmic systems that form AI and its future. The algorithms used are enhancing companies' speed and efficiency in defining their target groups and also the accuracy of decision-making. This last part will be the main subject in the analysis that will follow. We will try to cover all the arguments around AI and automated decision-making, especially under the scope of the rules defined by GDPR and the impact it has (or not) on the field of AI.

Amidst the cacophony of concerns over AI taking over jobs and the world in general, and cheers about what it can do to increase productivity and financial gains of companies, the potential for AI to actually be useful and do good can be overlooked. There is no doubt that the evolution of AI has brought positive outcomes in several areas and, generally, for mankind. One of the most important examples is the application of AI in biomedicine, including disease diagnostics, living assistance, biomedical information processing, and biomedical research.

The central objective of this analysis will be to point out the main impact of the GDPR on AI and the automated decision-making ruled by Article 22 of the GDPR. In the first part, we will refer to AI as a new reality and seek to frame and define it from an ethical perspective. We will be covering the GDPR's legal framework and the data protection regulations according to the European legal framework, while taking a closer look at the nature of personal data and automated decision-making. In the third part, we will focus on the legal context of Article 22, and we will refer to the vigorous discussions concerning the existence or not of a right of explanation. Finally, we will be analysing not only the risks, but also the opportunities of AI. Are we, after all, in favour or against dehumanisation?

2. WHAT IS ARTIFICIAL INTELLIGENCE?

No doubt AI is progressively escalating in its influence worldwide and is revolutionising business processes in such a manner that is no longer only

[5] See more un Bernard Marr, "8 Powerful Examples Of AI For Good", Forbes, February 2020 Available at: https://www.forbes.com/sites/bernardmarr/2020/02/10/8-powerful-examples-of-ai-for-good/?sh=1dcd13f0d18a.

in theory or science fiction — rather tangible and immediate.[6] AI raises a number of concerns with regard to ethical dilemmas, security, legal responsibilities. In this chapter, we will attempt to cover the definition of AI in order to have a better view on our analysis devoted to the impact of the European legislation on AI and automated decision-making.

As Russel and Norwig pointed out, "humankind has given itself the scientific name *homo sapiens*, which is translated as the "man the wise", because our mental capacities are so important to our daily lives and our sense of self. Philosophers, since ancient times, have tried to understand how seeing, learning, remembering, and reasoning could, or should, be done".[7] As it is well-known, AI was formally initiated by 1950 when Alan Turing proposed the 'Turing test', in which a machine would be deemed to exhibit intelligence. If it could engage in a text conversation that fooled a human into thinking, the machine would also be human.[8]

The term AI contains an explicit reference to the notion of intelligence. Since machine intelligence is a vague concept, although studied at length by psychologists, biologists, and neuroscientists, AI researchers use mostly the notion of rationality, which refers to the ability to choose the best action to take in order to achieve a specific goal, given certain criteria to be optimized and the available resources. Rationality is not the only element in the concept of intelligence, but it is an important part of it.

The definition of AI that we can find in the Oxford English Dictionary,[9] which is the most generic and traditional one, emphasizes the tasks performed by computer systems that normally require intelligence when done by humans. Research in AI has chiefly focused on the following elements of intelligence: learning, reasoning, problem-solving, perception, and language-understanding.[10] Ray Kurzweil refers to AI from a broad perspective, as the endeavour to design machines that execute functions that require in-

---

[6] Eric Winston, "GDPR — How does it impact AI? Information age", Data Protection and Privacy, 19 June 2019, Available at: https://www.information-age.com/gdpr-impact-ai-123483399/, (Last accessed: 05.09.2021).

[7] Stiuart Russell; Peter Norvig, *Artificial Intelligence: A Modern Approach*, Prentice Hall, 3rd edition, 2009, page 3.

[8] Alan Turing, *Computing Machinery and Intelligence*, Mind, Volume LIX, Issue 236, October 1950, pages 433-460.

[9] The definition of Artificial Intelligence is the following: "the study and development of computer systems that can copy intelligent human behaviour", Available at: https://www.oxfordlearnersdictionaries.com/definition/english/artificial-intelligence?q=artificial+intelligence, (Last accessed: 05.09.2021).

[10] Jake Copeland, "What is AI?", Alanturing.net., May 2000, Available at: http://www.alanturing.net/turing_archive/pages/reference%20articles/what%20is%20ai.html, (Last accessed: 05.09.2021).

telligence when performed by people.[11] AI strives to build intelligent entities as well as to understand them.

The European Commission's Communication on Artificial Intelligence (European Commission, 2018a)[12] defines AI as follows:

> "Artificial Intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things[13] applications)."

The High-Level Expert Group[14] defines the scope of research in AI:

> "As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)."

Generally, AI is defined as intelligence demonstrated by a machine and its ability to display human-like capabilities such as reasoning, learning, planning and creativity. We are referring to a software program with a set of

---

11 Stiuart Russell, Peter Norvig, *Artificial Intelligence: A Modern Approach*, Prentice Hall, 3rd edition, 2009, page 3.

12 European Commission (2018b). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions — Coordinated Plan on Artificial Intelligence (COM(2018) 795 final). Available at: https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence, (Last accessed: 05.09.2021).

13 The concept of the Internet of Things (IoT) refers to an infrastructure in which billions of sensors embedded in common, everyday devices – "things" as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities. As the IoT relies on the principle of the extensive processing of data through these sensors that are designed to communicate unobtrusively and exchange data in a seamless way, it is closely linked to the notions of "pervasive" and "ubiquitous" computing. Former Article 29 Data Protection Working Party adopted by European Data Protection Board, Opinion 8/2014 on the Recent Developments on the Internet of Things, page 4. Available at: https://www.dataprotection.ro/servlet/ViewDocument?id=1088, (Last accessed: 06.09.2021) and European Data Protection Supervisor, Opinion 7/2015 – Meeting the challenges of big data: a call for transparency, user control, data protection by design and accountability, page 7, Available at: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf, (Last accessed: 06.09.2021).

14 High-Level Expert Group on Artificial Intelligence, "A definition of AI: Main capabilities and scientific disciplines", 2019, page 2.

algorithms that mimic the cognitive functions of the human mind.[15] AI enables technical systems to perceive their environment, deals with what they perceive, solves problems and acts to achieve a specific goal. The computer receives data — already prepared or gathered through its own sensors such as a camera — processes it and responds.[16] One of the capabilities of AI is 'profiling', which is the ability of a software program or machine to take in data points about a particular person or subject and draw logical conclusions about that person or subject. This is the main aspect of AI that we will be looking into in our analysis.

2.1. LEGAL BASIS ON PRIVACY, AI AND THE NECESSITY OF AN ETHICAL FRAMEWORK

It is well known that AI currently encompasses a huge variety of subfields, from general-purpose areas such as perception and logical reasoning, to specific tasks such as playing games and diagnosing diseases. The vast majority of the AI advancements and applications we hear about refer to a category of algorithms. For the algorithms to work, they analyse massive amounts of data in order to find patterns. The question that arises concerning data protection is, if the users know that their privacy and the personal information that they are sharing is not being properly protected by the companies, would this factor make the users more reluctant to share information on the online platforms or applications that they use?

Futurist Kurzweil has made a host of predictions, some inspirational, others downright alarming. One of them is the sci-fi-sounding and dystopian notion that suggests artificial intelligence will one day become more powerful than human intelligence and improve itself at an exponential rate, otherwise known as 'the singularity'.[17] [18]

It is difficult to deny that AI is dominating our daily lives. Modern technologies and AI communities will need to consider the ethical and social implications of their work as AI comes to shape more realms of our life, from healthcare to financial markets. Ethical concerns abound in relation to the

---

[15] Eric Winston, "GDPR — How does it impact AI?", Information Age, Data Protection & Privacy, 19 June 2019, Available at: https://www.information-age.com/gdpr-impact-ai-123483399/, (Last accessed: 05.09.2021).

[16] European Parliament, What is artificial intelligence and how is it used?, Society, Updated March 2021, Available at: https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used, (Last accessed: 06.09.2021).

[17] Bryan Lufkin, "10 grand challenges we'll face by 2050", BBC, July 2017, Available at: https://www.bbc.com/future/article/20170713-what-will-the-challenges-of-2050-be, (Last accessed: 05.09.2021).

[18] Vernor Vinge, "Technological Singularity, Whole Earth Review, Winter Issue, 1993, Available at: https://frc.ri.cmu.edu/~hpm/book98/com.ch1/vinge.singularity.html, (Last accessed: 05.09.2021).

impact of AI on humanity, whether it is driverless cars taking life or death decisions on the roads or robots replacing human jobs.[19]

In order to assess the legal and ethical issues that are surging from AI and personal data, we need to understand how our privacy is affected by the development and application of AI. The Norwegian Data Protection Authority (DPA)[20] believes it to be imperative that we further our knowledge about the privacy implications of AI and discuss them, not only in order to safeguard the right to privacy of the individual, but also to meet the requirements of society at large. When an AI software is used by people and, more specifically, when a decision is made for them automatically, it is vital to ensure that the values of the person or subject are in focus at all times and protected.[21]

Many ethical and moral challenges are being raised, because of the lack of a common ethical framework. Businesses and public authorities should use AI with respect for the relevant legislation and the rights of the citizens. The use of intelligent systems should be lawful, fair and transparent. The statement of the European Group on Ethics in Science and New Technologies[22] highlighted the ethical principles and democratic prerequisites, such as respect for human dignity and the autonomy of the human being to control autonomous systems. The principle of responsibility means that 'autonomous' systems should only be developed and used in ways that serve the global social and environmental good, as determined by the outcomes of deliberative democratic processes.

Privacy and data protection laws are with no doubt the key area of law dealing with the effects of machines on our society.[23] One of the core issues appearing from the excessive use of autonomous intelligent systems, is whether the users have control over their personal data and the information they are sharing. Are we capable of maintaining control over our personal data and their use? In an age of ubiquitous and massive collection of data

---

19 Michael Butterworth, *The ICO and artificial intelligence: The role of fairness in the GDPR framework*, Computer Law & Security Review: The International Journal of Technology Law and Practice, 2018, Available at: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf, (Last accessed: 05.09.2021).

20 Datatilsynet, "Artificial Intelligence and Privacy – Report", The Norwegian Data Protection Agency, January 2018, page 5. Available at: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf, (Last accessed: 05.09.2021).

21 The Danish Government, "National Strategy for Artificial Intelligence. Ministry of Finance and Ministry of Industry, Business and Financial Affairs." page 7, 2019 Available at: https://eng.em.dk/media/13081/305755-gb-version_4k.pdf, (Last accessed: 05.09.2021).

22 European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems, European Union, Brussels 2018, pages 16-19, Available at: https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf, (Last accessed: 05.09.2021).

23 Michael Butterworth, *The ICO and artificial intelligence: The role of fairness in the GDPR framework*, Computer Law & Security Review 34, 2018, page 257–268.

through digital communication technologies, the right to protection of personal information and the right to respect for privacy are crucially challenged.

Both physical AI robots as part of the Internet of Things, as well as AI softbots that operate via the World Wide Web, must comply with data protection regulations, and not collect and spread data or be run on sets of data for whose use and dissemination no informed consent has been given. The systems that are generating automated decisions within an AI environment must not interfere with the right to private life and with the right to one's character.

According to Article 26, paragraphs 1 and 2, *in fine,* of the Constitution of the Portuguese Republic (henceforth CPR), the right to reserve the privacy of private life (the right to privacy) refers to a double dimension encompassing both the limitation of access and the limitation of sharing information related to private and family life, which is also provided for in article 80 of the Portuguese Civil Code.[24] Both dimensions are guaranteed within the scope of the CPR itself, always in compliance with the principle of proportionality, in Articles 34 and 35 as well as in the Portuguese Civil Code, Articles 75 to 78. Concerning paragraph 2 of Article 26 of the CPR, there is also protection provided by law and, more particularly, the personal data protection Law No. 58/2019, 8th August, which ensures the implementation of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016, into the Portuguese legal system, the on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR); and, finally, there is also protection of the referred dimensions provided by Articles 7 and 8 of the EU Charter of Fundamental Rights.

Despite the fact that the right to one's character is not specifically listed in Civil Code (henceforth CC), it is included in the general clause of the right of personality, as established in the Article 70 of the CC,[25] "general protection of personality". The general right of personality is truly a right to the free development of the personality and protects the personality in its evolution.[26] It is important to point out that it would be impossible to list all personality rights — so unlimited as unlimited are the personality dimensions —,[27] since they include, among others, the right to life, to freedom, to dignity, to name, to

---

[24] J.J. Gomes Canotilho; Vital Moreira, *Constituição da República Portuguesa anotada*, vol. I. 4.ª ed. rev. Coimbra: Coimbra editora 2014, page 467.

[25] SECTION II Personality rights Article 70 (General personality guardianship)

1. The law protects individuals against any unlawful offense or threat of offense to their physical or moral personality.

2. Regardless of the civil liability that may arise, the person threatened or offended may request the measures appropriate to the circumstances of the case, in order to avoid the consummation of the threat or mitigate the effects of the offense already committed.

[26] Orlando de Carvalho, *Teoria geral do direito civil,* Coimbra Editora, 2012, page 203.

[27] Orlando de Carvalho, *Teoria Geral do Direito Civil*, Coimbra Editora, 2012, pages 191,203, 231-232.

intimacy. The right to one's character includes the right not to be subject to non-consented assessments,[28] and as well as the right of personal identity are threatened from profiling. Orlando is listing the right to one's character, as an autonomous and special personality right, that protects the individuals against unauthorized evaluations of their character, that nowadays due to profiling techniques that they individuals are not aware of.[29]

Leite Campos asserts that personality rights are those "which are an attribute of the person himself and whose object is the property of his physical, moral and legal personality, as emanations or manifestations of the personality, in general", rights which[30] "serve to allow and assure man to achieve what he is, against or beyond his own idea of self-realization".[31] By protecting the development of personality, a right to individual freedom is enshrined in relation to the constitution of personality, integrating a "right to difference", saying that "the problem, deep down, is to allow each one to choose their way of life, as long as it does not harm third parties".[32]

Concerning the necessity of the existence of an ethical framework, the High-Level Expert Group on AI, in 2019, presented Ethics Guidelines for Trustworthy Artificial Intelligence.[33] Most specifically, the use of AI should be:

> Lawful: The use of AI should be in respect of all applicable laws and regulations.
>
> Ethical: Respecting ethical principles and values.
>
> Robust: Both from a technical perspective while taking into account its social environment.

Therefore, it is more than necessary to create clear boundaries and exact criteria in order to have mechanisms that ensure ethical development and ethically correct application of 'autonomous' intelligent systems. In light of concerns with regard to the implications of 'autonomous' systems on private life and privacy, consideration may be given to the ongoing debate about the

---

[28] Maria Raquel Guimarães, *A tutela da pessoa e da sua personalidade como fundamento e objecto da disciplina civilística, Algumas questões,* Estudos comemorativos dos 20 anos da FDUP, 2017, page 305-307.

[29] Orlando de Carvalho, *Teoria geral do direito civil,* Coimbra Editora, 2012, note 69, pages 265-266.

[30] Diogo Leite Campos, Nós – Estudos sobre o Direito das Pessoas., Coimbra: Almedina, 2004, page 54.

[31] Diogo Costa Gonçalves, *Pessoa e Direitos de Personalidade – Fundamentação Ontológica da Tutela*, Coimbra: Almedina, 2008, page 93.

[32] Paulo Mota Pinto, *O Direito ao Livre Desenvolvimento da Personalidade*, in Boletim da Faculdade de Direito de Coimbra, Portugal-Brasil ano 2000, Coimbra Editora, 1999, pages 158-160.

[33] Ethics guidelines for trustworthy AI, Report/Study, Shaping Europe's digital future, April 2019, Available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai, (Last accessed: 05.09.2021).

introduction of two new rights: the right to meaningful human contact and the right to not be profiled, measured, analysed, coached or nudged.[34]

In view of the countless possibilities for the processing of personal data by public and private entities in terms of access, collection, storage and information traffic, as Miranda and Medeiros are stating, it is urgent to protect this data by removing illegitimate intrusions in the sphere of individuals' private lives.[35] In this sense, the extravagant hypothesis that, for example, a Machine-Learning algorithm could autonomously decide on the creation of a single national number for each person, would simply not be acceptable. In fact, the use of AI cannot escape the observance of the scope of the protection scope of the right to personal data computer processing,[36] provided at national level, in Articles 26, 35 and 18 of the CPR and in Law n.º 58/2019, of 8th August, nor can it fail to observe the list of principles that result from them, and also at EU law level, in Articles 7, 8, 11 and 52 par. 1 of the European Union Charter of Fundamental Rights (henceforth EUCFD), and in Regulation (EU) 2016/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, in Directive 2002/58/EC,[37] concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and Directive 2000/31/EC,[38] on certain legal aspects of information society services, in particular electronic commerce in the Internal Market ("Directive on electronic commerce").

2.2. ARTIFICIAL INTELLIGENCE, MACHINE-LEARNING, ALGORITHMS AND BIG DATA

During the last decade, Machine-Learning — as one of the subparts of AI — has been growing and developing rapidly. Practical applications of Machine-Learning include image and speech recognition, such as person-

---

[34] European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems, European Union, Brussels 2018, page 17, Available at: https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf, (Last accessed: 05.09.2021).

[35] Rui Medeiros; Jorge Miranda, *Constituição Portuguesa Anotada*, Tomo I, Coimbra: Coimbra Editora. Art.º 35.º, note III, 2005, page 379-380.

[36] José A.R.L. González, "Responsabilidade por danos e Inteligência Artificial (IA). Revista de Direito Comercial ``. 4, 2020 pages 29-30, Available at: https://www.revistadedireitocomercial.com/responsabilidade-por-danos-e-inteligncia-artificial-ia, (Last accessed: 05.09.2021).

[37] Law no. 41/2004 of 18 August, amended by the Law no. 46/2012 of 29 August, concerning the processing of personal data and privacy in electronic communications sector (Directive 2002/58/EC on privacy and electronic communications)

[38] Law no. 7/2003 of 9 May, amended by Decree-Law no. 62/2009 of 10 March and Law no. 46/2012 of 29 August , (Directive 2000/31/EC on certain legal aspects of information society, in particular electronic commerce, domestic (...)).

al assistance softwares.[39] Another example of natural language processing that can be used in translation (for example, automated entitling) or in extracting diagnostic information from free-form physician notes,[40] predictive analytics, which is a branch of data mining,[41] are also some main examples of Machine-Learning based applications. The development of those digital systems improves their performance on a given task, over time, through experience.[42] AI involves machines that are using statistics to find patterns in large amounts of data and that, at the same time, evolve the ability to perform repetitive tasks with data, without the need for constant human guidance and intervention.

It is essential to understand that algorithms are processed and expressed through programming languages, thus becoming machine-executable software programs.[43] An algorithm can be very simple, such as detecting the order of numbers or arranging lists of words in alphabetical order. However, they can also be very complex, such as the encryption of files or the speech recognition algorithms.

Algorithms are logical systems whose origins are as ancient as mathematics. In mathematics and computer science, an algorithm is a self-contained step-by-step set of operations to be performed. Algorithms perform calculation, data processing, and/or automated reasoning tasks.[44] We understand, therefore, that not all algorithms involve AI, but every AI system

---

39 Amazon's Alexa and Apple's Siri are the most used ones.

40 Laura Hamilton, "Six Novel Machine Learning Applications", Forbes, January 2014, Available at: https://www.forbes.com/sites/85broads/2014/01/06/six-novel-machine-learning-applications/?sh=1c16ad981060, (Last accessed: 05.09.2021).

41 'Data mining is the process of analysing data from different perspectives and summarising it into useful new information. Data mining software is one of a number of tools for interrogating data. It allows users to analyse data from many different dimensions or angles, categorise it, and summarise the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases. It is commonly used in a wide range of profiling practices, such as marketing, surveillance, fraud detection and scientific discovery. Obviously, for data mining to be effective it is necessary to analyse large amounts of previously collected data.', European Data Protection Supervisor, Available at: https://edps.europa.eu/node/3099#data_mining, (Last accessed: 05.09.2021).

42 Inês Silva Costa, *A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas*, Revista Electrónica De Direito, No 1, (VOL. 24) February 2021, page 38, Available at: https://cije.up.pt/pt/red/edicoes-anteriores/2021-nordm-1/a-protecao-da-pessoa-na-era-dos-big-data-a-opacidade-do-algoritmo-e-as-decisoes-automatizadas/, (Last accessed: 05.09.2021).

43 Mihalis Kritikos, "The impact of the General Data Protection Regulation (GDPR) on artificial intelligence", EPRS | European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 641.530 – June 2020, page 3, Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf, (Last accessed: 05.09.2021).

44 Computer Science Wiki Algorithms, https://computersciencewiki.org/index.php/Algorithms, (Last accessed: 05.09.2021).

is based on algorithms. The combination of two factors that have emerged in the course of the information society, whose front we will seek to deepen, illustrates why their applications in the real world are proliferating and why they are placed at the heart or basis of the desire for complex software.

An algorithm, in the strict sense of the term, is the description of a finite and unambiguous sequence of steps or instructions for producing results, an output from initial data, the input. Machine-Learning is when we educate an algorithm through a systematic process,[45] for example to identify a person or a car every time they appear in a photo. This deep learning lets computers "see" and distinguish objects and texts in images and videos. This is possible only by feeding the algorithm with data inputs. Data encompasses a lot of things—numbers, words, images, clicks. If it can be digitally stored, it can be fed into a Machine-Learning algorithm.

AI is nothing without data. Machine-Learning algorithms are probabilistic because their output is always changing, depending on the learning basis and the data that they are given. In order to comprehend why AI needs huge volumes of data, it is necessary to understand how the system learns and which are the main three steps. Developing AI requires the input of experiential data. Machine-Learning generally proceeds firstly by selecting the information that contains patterns or similarities. Then those patterns found in the information collected are identified. Those two steps generate a model that can recognise the patterns that emerge when fresh data is processed by the model.[46]

The introduction of Machine-Learning into the market processes is resulting in the personalization of contractual conditions and products offered to the consumers. Those algorithms are accessing the information that we, as users of the various websites, are giving to the system as consumers. The patterns created and the appearing results are subject to personalisation and filtering of the algorithm used. These profiling and classification algorithms are responsible for the shaping and management of individuals and groups.[47]

As far as it concerns privacy issues that are relevant for our analysis, AI has two main aspects. The first one is when a system has the capability to make a decision itself without human interaction. The second aspect is when the system is developed by learning from experience. Since data is so central to contemporary AI development, several data-related concepts are frequently raised during debates about AI and the engineers spend as much

---

[45] Karen Hao, "What is machine learning?", MIT Technology Review, November 2018, Available at: https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart/, (Last accessed: 05.09.2021).

[46] Datatilsynet, "Artificial Intelligence and Privacy – Report", The Norwegian Data Protection Agency, January 2018, page 7, Available at: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf, (Last accessed: 05.09.2021).

[47] Luciano Floridi, "Big Data and their epistemological challenge.", Philosophy and Technology 25(4) 2012, pages 435-437, Available at: DOI 10.1007/s13347-012-0093-4, (Last accessed: 05.09.2021).

time thinking about data as they do about algorithms.[48] The rise of Machine-Learning algorithms and the usage of Big Data has led to the creation of systems that lead to autonomous decisions. The automated decision-making algorithm is believed to be a subpart of AI, where no human interaction is needed in order to make a decision.[49]

Reis[50] refers to the fact that the multiplication of the application of algorithms in the real world is based on the combination of two factors that have emerged in the course of the information society. The first was the extension of the capacity of computer-processing, which accelerated the speed of the execution of complex tasks by computers. The second factor was the advent of Big Data, the bargaining and storage of gigantic amounts of information, which gave the algorithms the possibility to identify imperceptible patterns with human eyes, in activities of any kind in digital environments. This is the actuation field of algorithms, that covers AI, Machine-Learning, Deep Learning, Neural Networks and the Internet of Things.

Big data is characterized by the three V's: high-volume, high-velocity and/or high-variety. Information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision-making, and process automation.[51] Those data can be structured or unstructured. Theoretically, unstructured data could be analysed only by humans.[52] The use of Big Data does not revolve around how much data you have, but what you do with it. These datasets are so large and complex because of the different sources that are mined. They can be in various formats and the authenticity and accuracy of these data can vary. It is obvious that AI engineers need good quality of data in order to perform Machine-Learning algorithms and test the results. They can be examined and analysed for insights that lead to better decisions and strategic business moves.[53] Depending on the circumstances, the use of this data can be unreliable, unethical, and even

---

48 Philip Boucher, *Artificial intelligence: How does it work, why does it matter, and what can we do about it?*, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), June 2020, page 8 Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf, (Last accessed: 05.09.2021).

49 Argyro Karanasiou; Dimitris Pinotsis, "A Study into the Layers of Automated Decision Making: Emergent Normative and Legal Aspects of Deep Learning." International Review of Law, Computers & Technology., 2016, Available at: DOI: 10.1080/13600869.2017.1298499.

50 Paulo Victor Alfeo Reis, *Algoritmos e o direito*, São Paulo : Almedina, 2020, page 21.

51 Big Data definition, Gartner Glossary, Information Technology Glossary, Available at: https://www.gartner.com/en/information-technology/glossary/big-data, (Last accessed: 05.09.2021).

52 See more on the article "O que é Big Data?", Canaltech, Big Data, Available at: https://canaltech.com.br/big-data/o-que-e-big-data/, (Last accessed: 05.09.2021).

53 "Big Data, What it is and why it matters", Big Data Insights, SAS, Available at: https://www.sas.com/en_us/insights/big-data/what-is-big-data.html, (Last accessed: 05.09.2021).

illegal.[54] In particular, the connection with analytics and AI makes Big Data specifically relevant to data protection. From a legal aspect, as Hildebrandt states, notably when referring to location data, what is crucial is if those data are related to an identified or identifiable natural person because this constitutes the "personal data "under the European legal framework.[55]

In their combination, AI and Big Data are becoming part of business for not only private but also public organisations. According to Zarsky, Big Data, apart from the scepticism, is generating great interest. Many firms needed to accelerate their adaptation to the new data environment. Therefore, "*law and policy can no longer ignore the incremental changes that have brought about this new digital era. Rather, they must provide responses to this change—be it a 'revolution', or a mere 'evolution'.*"[56]

3. AUTOMATED DECISIONS AND THE PROTECTION OF PERSONAL DATA UNDER THE GDPR

3.1. ALGORITHMIC DECISION-MAKING AND EU DATA PROTECTION

The vigorous data protection framework of GDPR was the necessary step in the right direction as it empowers individuals to regain ownership of their personal data. The birth of data protection in Europe started in the 70's, when the usage of new technologies appeared. The rapid advancement in the area of electronic data processing and the first appearance of mainframe computers that started being used in public administration as well as in private enterprises set up extensive data banks to improve the collection, process and share of personal data and information. The new developments and technological advancements in the telecommunications field facilitated, at the same time, the international transborder flows of data.

The rapid expansion of Internet usage and the autonomous nature of AI brought challenges and the legislation of the European Union was called to accompany it rapidly. The new legal framework of these new standards had to find the right balance between the protection of freedom and data

---

[54] Philip Boucher, *Artificial intelligence: How does it work, why does it matter, and what can we do about it?*, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), June 2020, page 8 Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf, (Last accessed: 05.09.2021).

[55] Mireille Hildebrandt, "Location Data, Purpose Binding and Contextual Integrity: What's the Message?" contribution to Floridi, Luciano, Protection of Information and the Right to Privacy — A New Equilibrium?, Chapter 3, Law, Governance and Technology Series Volume 17 Springer, 2014, page 6, Available at: https://works.bepress.com/mireille_hildebrandt/54/, (Last accessed: 05.09.2021).

[56] Tal Z. Zarsky, "Incompatible:The GDPR in the Age of Big Data", Seton Hall Law Review, Vol. 47:995, 2017, pages 1000-1001.

protection and the embracement of the advantages of the digital economy. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108") was adopted by the Council of Europe and was the first legally binding international instrument in the area of data protection. The "Convention 108" took the view that those holding and using personal information in computerised form have a social responsibility to safeguard such personal information. Decisions that affected individuals at that time were based more and more on information stored in computerised data files.[57]

The Directive 95/46/EC, linked to the technological developments of the 70's, was repealed by the GDPR. It is important to underline at this point that the GDPR is not specifically addressing AI. Although the complex digital environments have been taken into account by the new European legal framework, the regulator chose to adhere explicitly to technological neutrality.[58] This neutrality is balancing the fact that technology has been moving in very rapid rhythms in recent years, faster than the law. Hence, the Regulation is mainly regulating the effects produced and not the technology used for data processing and, therefore, the rules and principles can be flexible enough to cover future technological changes and confer lasting protection.

In particular, AI gives reasons to focus on the potential risks arising from its use as well. The risks to be dealt with are mainly based on autonomous systems that have self-learning capacities which allow them to undertake or omit certain actions which are not necessarily predictable in advance and may, therefore, create undesirable results leading to injury or damage to their users.[59]

One of the main effects of the dissemination of algorithms in computing was the impulse or desire of AI, as previously underlined, a field of study created in the 1950s that develops mechanisms capable of simulating human reasoning. Using more and faster computational calculations with which statistical comparisons can be made, machines have gained the ability to modify their function from the accumulated experience and to improve their

---

[57] Eduardo Ustaran, *European Data Protection: Law and Practice*, IAPP Publication, International Association of Privacy Professionals, 2018, page 11.

[58] In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. 2The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. 3Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation., General Data Protection Regulation, Recital 15, Available at https://gdpr-info.eu/recitals/no-15/, (Last accessed: 05.09.2021).

[59] Sebastian Lohsse; Reiner Schulze; Staudenmayer Dirk, *Liability for artificial intelligence and the Internet of things* / ed. lit. , Münster Colloquia on EU law and the Digital Economy IV, Hart Publishing, Nomos, 2019, page 12.

performance, in an associative process that mimics learning.[60] Therefore, next to the benefits of digital technologies, the reality of collecting, processing, storing and using data has brought new and quite unknown risks.[61]

The right not to be subject to automated decision-making of Article 22 of GDPR is applied to the phase of AI development and its use in analysing and decision-making about individuals and the effect of outcomes from its use. As we also mentioned above, the combination of AI automated systems and Big Data enabled automated decision-making, even in domains that require complex choices, based on multiple factors and non-predefined criteria. In some cases, those algorithmic systems are not only cheaper, but also more precise and impartial than human ones.[62] Apart from the advantage of efficiency, we cannot foresee the risks of algorithmic discrimination and the mistakes that can be driven therefrom.

3.2. THE CONCEPT OF PERSONAL DATA IN THE GDPR

In GDPR, the main protagonist, as it is obvious, is the personal data concept. The definitions of the core notions are intentionally broad. Indeed, personal data are defined broadly and therefore, they can apply in any complicated software and application of AI. The online reality that the law tries to accompany with elasticity seems to be aligned with the personal data definition. The information requirements established by the GDPR can be met with regard to AI-based processing, even though the complexity of AI applications has to be taken into account.

The importance of the definition of personal data is crucial for AI and our analysis. Numerous AI applications process personal data, especially under processes that are fully automated and which have significant consequences for the data subjects. On the one hand, personal data may contribute to the data sets used to train machine-learning systems, namely to build their algorithmic models. On the other hand, such models can be applied to personal data to make inferences concerning individuals.

a) The general definition

The Regulation on Article 4(1) includes the definition of personal data, as follows: *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is*

---

60 Paulo Victor Alfeo Reis, *Algoritmos e o direito*, São Paulo : Almedina, 2020, page 169.

61 Mira Burri; Rahel Schär, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, Journal of Information Policy, Vol. 6 June 2016, pages 479-511, Available at SSRN: https://ssrn.com/abstract=2792222 or http://dx.doi.org/10.2139/ssrn.2792222, (Last accessed: 05.09.2021).

62 Giovanni Sartor, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, EPRS | European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 641.530 – June 2020, page 21.

one who can be identified, directly or indirectly". In other words, any information that is clearly about a particular person. The European data protection law does not cover data processing which concerns legal persons, and in particular, does not concern undertakings established as legal persons, including the name and form of the legal person and their contact details. Examples of personal data as referred to in Article 4(1) are "..an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

The concept of personal data, well consolidated in the European and international space, is broken down into four different and autonomous elements.[63] Those elements are also established by Former Working Party 29's Opinion 4/2007 (WP29) that until today remains relevant.[64] The WP29 set out four 'building blocks' of the definition of personal data which are 'any information', 'relating to', 'an identified or identifiable' and 'natural person'.

b) 'Any information'

As it is referred to on WP29, the term 'any information' contained in the Directive markedly signals the willingness of the legislator to design a wide concept of personal data. This wording calls for a broad interpretation.

The first building block of 'any information' has three main aspects in order to be considered as personal data and these are its nature, content and format. Concerning its nature, any type of statement about a person, objective and subjective, may be considered as personal data. Subjective statements are the ones that express one's opinions or an assessment. It is also necessary to note that information does not need to be true or proven.

The content of personal data includes any sort of information, and it is not limited only to private and family life, *stricto sensu*, but also information regarding whatever type of activity undertaken by the individual, like information about working relations or the economic or social behaviour. The Court of Justice of the European Union (CJEU) in its jurisprudence has established that private and family life must be widely interpreted.[65] Nevertheless, we

---

[63] António Barreto Menezes Cordeiro, *Direito da proteção de dados : à luz do RGPD e da Lei n.º 58/2019* , Coimbra : Almedina, 2020, page 107.

[64] Former Article 29 Working Party Opinion 4/2007 on the concept of personal data, European Data Protection Board, Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, (Last accessed: 05.09.2021).

[65] Judgement of the European Court of Human Rights in the case Amann v Switzerland of 16.2.2000, §65: "[...] the term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life" (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pages 33-34, § 29, and the Halford judgment cited above, pp. 1015-16, § 42). That broad interpretation corresponds

need to underline and distinguish the object of the right to privacy and the right to data protection: not all personal data refer to privacy and not all information relating to privacy is personal data.

The concept of personal information, widely, goes beyond the meaning that is traditionally attributed to it within the personality right to privacy, even if a more flexible conception is assumed, as the ECHR does. As Cordeiro mentions, "*private life covers everything that is not public and professional or social*."[66] Also, the protection of the legal regime of Article 80 of the Civil Code is not the same as the one in the concepts of Personal Data Protection Law. More specifically the European Court of Justice (CJEU) stated in the judgement of the case ClientEarth V. PAN Europe, "*the fact that information is provided as part of a professional activity does not mean that it cannot be characterised as a set of personal data.*"[67] [68]

It should be noted that the Charter of Fundamental Rights of the European Union (CFR) enshrines the protection of personal data in Article 8 as an autonomous right, separate and different from the right to private life referred to in Article 7. As Recital 30 explains, information that constitutes an 'online identifier'. For instance, an IP address can be used to identify a person and create their profile,[69] showing the broadness of content that is considered personal data.

Considering the format or the medium in which that information is contained, GDPR is applied independently of the form that includes the information available, for instance, on paper or computer, be it alphabetical, numerical, graphical, photographical, or acoustic. This is a logical consequence of covering the automatic processing of personal data within its scope.

c) 'Relating to'

The second building block of the definition 'relating to' is crucial as it is very important to precisely find out the links that matter and how to distin-

with that of the Council of Europe's Convention of 28 January 1981 [...]", Available at: http://hudoc.echr.coe.int/eng?i=001-58497, (Last accessed: 05.09.2021).

66 António Menezes Cordeiro, *Tratado de Direito Civil,* Vol. IV, Coimbra: Almedina, 5ª ed., 2019, page 267.

67 Judgement of CJEU, C-615/13P, ClientEarth v PAN Europe, paragraph 30.

68 see, to that effect, the Judgments of CJEU in Österreichischer Rundfunk and Others, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 64; Commission v Bavarian Lager, C-28/08 P, EU:C:2010:378, paragraphs 66 to 70; and Worten, C-342/12, EU:C:2013:355, paragraphs 19 and 22).

69 1.Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. 2. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them., General Data Protection Regulation, Recital 30, Available at: https://gdpr-info.eu/recitals/no-30/, (Last accessed: 05.09.2021).

guish them. Information can be considered to "relate" to an individual when it is about that individual, but in many situations, this relationship cannot be easily established, let alone in AI applications that use algorithms that process data leading to automated decisions.

On certain occasions, the information conveyed by the data concerns objects and not individuals. The objects usually belong to someone or may be subject to particular influence by or upon individuals. For example, the price of a car that belongs to an individual may be personal data since it can indirectly determine his financial state or his tax obligations. Once we can establish a relationship between an individual and information about an object, this information becomes personal data.

The Opinion 4/2007 of WP29 considered that in order to establish the criteria of "relating to" the following three elements must apply: the 'content', the 'purpose' and the 'result' element.[70] The 'content' element corresponds to the most obvious and common understanding in a society of the word 'relate', for instance, when a person is subject to analysis or evaluation, as happens with exams results or health analysis results. The existence of the 'purpose' is established when the information is processed in order to analyse in a certain way or influence the status or behaviour of an individual, such as the payment of remuneration of a worker that can relate to his or her name.[71] Lastly, the 'result' element is present when the processing of data has an impact on a certain person's rights and interests. Those three elements must be considered as alternative conditions, and not as cumulative ones.

d) 'Identified or identifiable'

The Directive requires that the information relate to a natural person that is 'identified or identifiable'. Therefore, the third building block of Opinion 7/2007 in the WP29 states that, in general terms, a natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group. Accordingly, the natural

70 Article 29 Working Party Opinion 4/2007 on the concept of personal data, pages 9-12, European Data Protection Board, Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, (Last accessed: 05.09.2021).

71 Judgment of CJEU of Österreichischer Rundfunk and Others, Joined cases C-465/00, C-138/01 and C-139/01, 20 May 2003, paragraph 38: "The Commission adopts a similar position. At the hearing, it nevertheless submitted that the collection of data by the bodies subject to control by the Rechnungshof with a view to communication to the latter and inclusion in the report is itself within the scope of Directive 95/46. Collection serves not only the function of auditing but also, primarily, the payment of remuneration, which constitutes an activity covered by Community law, having regard to the existence of various relevant social provisions in the Treaty, such as Article 141 EC, and to the possible effect of that activity on the freedom of movement of workers."

person is 'identifiable' when, although the person has not been identified yet, there is a possibility to do it. That is the meaning of the suffix "-able".

The rise of Big Data, low storage costs and fast processing, but also the pairing of data, has made the identification of individuals more challenging than ever. Recital 26 offers guidance in this matter which refers to the term "identifiable" when it reads that "whereas to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person."[72] [73]

More specifically, Recital 26 addresses identifiability, namely, the conditions under which a piece of data that is not explicitly linked to a person still counts as personal data, since the possibility exists to identify the person concerned:

> "3. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. 4. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."

Through pseudonymisation, the data items that identify a person (i.e., the name) are substituted by a pseudonym, but the link between the pseudonym and the identifying data items can be re-traced by using separate information (e.g., through a table linking pseudonyms and real names, or through a cryptography key to decipher the encrypted names). Recital 26 of GDPR specifies that pseudonymised data are still personal data.[74] Personal data which have undergone pseudonymisation, attributable to a natural person by the use of additional information, should be considered to be information on an identifiable natural person.

The connection between the personal nature of information and technological development is mentioned in Recital 9 of Regulation 2018/1807:[75] "If technological developments make it possible to turn anonymised data into

---

[72] Article 29 Working Party Opinion 4/2007 on the concept of personal data, page 15, Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, (Last accessed: 05.09.2021).

[73] Recital 26 EU GDPR, Not Applicable to Anonymous Data, Available at: https://gdpr-info.eu/recitals/no-26/, (Last accessed: 05.09.2021).

[74] Giovanni Sartor, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Scientific Foresight Unit(STOA), Panel for the Future of Science and Technology, June 2020, page 35, Available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530, (Last accessed: 05.09.2021).

[75] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

personal data, such data are to be treated as personal data, and Regulation (EU) 2016/679 is to apply accordingly."

In connection with the GDPR definition of personal data, AI raises, most notably, two key issues. Firstly, the 're-personalisation' of anonymous data, namely the re-identification of the individuals to which such data are related and secondly, the inference of further personal information from personal data that are already available. As it has been argued, 'in any 'reasonable' setting, there is a piece of information that is in itself innocent, yet in conjunction with even a modified (noisy) version of the data, yields a privacy breach.'[76]

Hence, the crucial challenge concerning AI and the processing of personal data is connected to re-identifiability. Re-identification can occur as the result of algorithms tracking repetitive patterns.[77] Specifically, breaking patterns or cases that lie far from the majority can be related to a specific person, distinguishing it from the anonymous crowd. Consequently, the concept of "unidentifiable" data is fluid.

Thanks to AI and Big Data, pieces of data that apparently are unidentified, not being linked to a specific individual, may be re-identified, and reconnected to the individuals concerned. The re-identification of sensitive data may have serious consequences for the individual's rights and freedoms. As an example, we can imagine the cases in which de-identified medical records that have been made accessible to the public are re-identified at a later stage so that the public comes to know the medical conditions of the individuals concerned. Without a doubt, the recent COVID-19 pandemic spotlighted the urgent need of establishing a new legal framework around the processing of personal data by AI software, especially when related to health medical records used by public authorities. During the pandemic, we need to underline the fact that data is beyond doubt playing a key role and is the lifeblood of AI.[78]

e) 'Natural Person'

Concluding, the fourth building block refers to the 'natural persons'. The protection of the Directive is applied to human beings and therefore, the right to the protection of personal data is, in that sense, a universal one that is

[76] Cynthia Dwork, Moni Naor†, "On the Difficulties of Disclosure Prevention in Statistical Databases or The Case for Differential Privacy", Journal of Privacy and Confidentiality, 2, Number 1, 2010, pages 93–107, 2010, page 93.

[77] Natalia Criado; Jose M. Such, "Digital discrimination", Algorithmic Regulation, Oxford University Press, 2019, page 11, Available at: https://www.researchgate.net/publication/336792693_Digital_Discrimination, (Last accessed: 05.09.2021).

[78] Reinier Schlatmann, "COVID-19 and beyond: AI and health", Politico, October 2020, Available here: https://www.politico.eu/sponsored-content/covid-19-and-beyond-ai-and-health/, (Last accessed: 05.09.2021).

not restricted to nationals or residents in a certain country.[79] The protection is only granted during people's lives and not after their death, unlike what happens in Portuguese Law 58/2019 that regulates the GDPR in article 17.[80] The Data Protection Law extends the protections set out in the GDPR to deceased data subjects' special categories of personal data, as well as to personal data pertaining to private life, image, and communications. The deceased data subject's rights may be exercised by a person appointed by the deceased data subject or, in the absence of an appointed person, by the data subject's successors. The deceased data subject may also determine that those rights may not be exercised after his/her death.

There are numerous conceivable problems with this framework, including a lack of clarity about which formal criteria apply to the choice of nominating someone else to exercise personal data rights, and the decision to prevent those rights from being exercised after death. It is fairly vague if granting the right of access to a deceased data subject's personal data related to private life and communications is compliant with the Constitution, and it is also unclear whether a deceased data subject's right to bar the exercise of his or her personal data rights after death should outweigh his or her successors' right to succeed.[81]

The concept of a natural person is referred to in Article 6 of the Universal Declaration of Human Rights, according to which *"Everyone has the right to recognition everywhere as a person before the law"*. Every Member State legislation defines the concept of legal personality of human beings in civil law, which is understood as the capacity to be the subject of legal relations, starting with the birth of the individual and ending with his death.

---

[79] Recital 14 Not Applicable to Legal Persons

1.The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. 2This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person. Available at: https://gdpr-info.eu/recitals/no-14/, (Last accessed: 05.09.2021).

[80] Artigo 17.º Proteção de dados pessoais de pessoas falecidas

1 — Os dados pessoais de pessoas falecidas são protegidos nos termos do RGPD e da presente lei quando se integrem nas categorias especiais de dados pessoais a que se refere o n.º 1 do artigo 9.º do RGPD, ou quando se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações, ressalvados os casos previstos no n.º 2 do mesmo artigo. 2 — Os direitos previstos no RGPD relativos a dados pessoais de pessoas falecidas, abrangidos pelo número anterior, nomeadamente os direitos de acesso, retificação e apagamento, são exercidos por quem a pessoa falecida haja designado para o efeito ou, na sua falta, pelos respectivos herdeiros. 3 — Os titulares dos dados podem igualmente, nos termos legais aplicáveis, deixar determinada a impossibilidade de exercício dos direitos referidos no número anterior após a sua morte.

[81] Tiago Félix da Costa; João Alfredo Afonso, "Portugal-National GDPR Implementation Overview", May 2020, Available at: https://www.dataguidance.com/notes/portugal-national-gdpr-implementation-overview, (Last accessed: 05.09.2021).

4. THE ARTICLE 22 OF GDPR — A NEW ERA OF AUTOMATED-DECISION MAKING

Automated-decision making is ruled by Article 22 of the GDPR. The article provides a general prohibition on automated decision-making and, at the same time, introduces a broad phasma of exceptions that we will try to analyse in this chapter. While the GDPR offers new rights and protection, their scope and limits are open to debate, partly due to the clumsy syntax of the relevant articles and the lack of authoritative guidance concerning their interpretation.

As previously said, thanks to AI, all kinds of personal data can be used to analyse, forecast and influence human behaviour. This algorithmic function turned the outcomes of processing data into valuable commodities. In particular, AI enables automated decision-making even in domains that require complex choices, based on multiple factors and non-predefined criteria. In many cases, automated predictions and decisions are not only cheaper, but also more precise and impartial than human ones, as AI systems can avoid the typical fallacies of human psychology and can be subject to rigorous controls.[82]

Moreover, the processing of non-sensitive personal data such as personality traits,[83] interests, financial situation, and other facts, can result in sensitive data, for instance, health data, depending on the AI methods and algorithms that are applied in the processing.[84] As a consequence, it is questionable whether the rights and legitimate interests of data subjects will be preserved, since there is no way to predict the outcome, for instance, the category of data that will be generated to apply the legal provisions regarding the processing of special categories of data.[85]

Article 22 of the GDPR provides that any personal data subjects shall have the right not to be exposed to decisions which, cumulatively:

---

82 Giovanni Sartor, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, Scientific ForesightUnit(STOA),| Panel for the Future of Science and Technology, June 2020, page 1, Available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530, (Last accessed: 05.09.2021).

83 Sonia See Roccas; Lilach Sagiv, "The Big Five Personality Factors and Personal Values", Sage Journals, Volume: 28 issue: 6, June 2002, Available at: https://journals.sagepub.com/doi/abs/10.1177/0146167202289008, (Last accessed: 05.09.2021).

84 Frederike Kaltheuner; Elletra Bietti, 2018. "Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR.", Journal of Information Rights, Policy and Practice, 2(2), page 4, Available at: DOI: http://doi.org/10.21039/irpandp.v2i2.45, (Last accessed: 05.09.2021).

85 Ioannis Iglezakis; Theodoros Trokanas; Panagiota Kiortsi, "The Right Not to Be Subject to Automated Individual Decision-Making/Profiling Concerning Big Health Data. Developing an Algorithmic Culture", March 2021, page 9, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3802771, (Last accessed: 06.09.2021).

1. Have been taken only based on automated processing of information concerning them (including, through the creation of profiles) and
2. Impact their legal sphere or affect them significantly.

This right can only be invoked if a decision is at stake that is considered necessary for the conclusion or execution of a contract between the data subject and a data controller. Lastly, this decision is authorized by the European Union or the member state legislation to which the person responsible for the treatment is subjected, as long as the treatment is accompanied by appropriate measures to safeguard the data subject's rights and is carried out based on the explicit consent of the data subject.

Automated decision-making has a different scope and may partially overlap with or result from profiling. The solely automated decision-making is the ability to make decisions by technological means without human involvement. Automated decisions can be based on any type of data, and it seems to encompass a multitude of decision types.[86] For instance, data provided directly by individuals concerned such responses as to a questionnaire, decisions on loan granting by a bank, conceding an insurance package, administrative decisions, data observed about the individuals such as location data collected via an application, derived or inferred data such as a profile of the individual that has already been created, like a credit score.

Therefore, we need to note that automated decisions can be made with or without profiling and vice versa. However, profiling and automated decision-making are not necessarily separate activities. Something that starts off as a simple automated decision-making process could become one based on profiling, depending upon how the data is used.

4.1 ARTICLE 22: "DECISION BASED SOLELY ON AUTOMATED PROCESSING"

Beyond the legal grounds of processing and the data protection principles, GDPR stipulates a number of responsibilities of the data controllers and the data subject's rights that are relevant to the AI algorithms. It is important to note that article 22 of GDPR is referring to "automated decision-making, including profiling".[87] The provision is formulated as the right of the data subject "not to be subject to a decision based solely on automated process-

---

[86] Maja Brkan, *Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond*, A revised version of this paper has been published in International Journal of Law and Information Technology, January 2019, page 3, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901, (Last accessed: 05.09.2021).

[87] GDPR is devoting a specific definition of the concept of profiling on article 4 par. 4 as follows: "'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;".

ing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".

Importantly, Article 22, like Article 15 before it, confers a very delimited right.[88] It only applies when a decision is based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects the data subject. The italicized wording sets a high threshold for triggering the restrictions in this article. Moreover, the stricter GDPR requirements of Article 15 are specifically linked to automated, individual decision-making and profiling that fall within the narrow scope of Article 22. These requirements include the existence of automated decision making, including profiling, meaningful information about the logic involved, and the significance and the envisaged consequences of such processing for the individual. The bottom line is that if Article 22 does not apply, these additional obligations do not apply either.

As Palmela Fidalgo also highlights, Article 22 came to prohibit the usage of the results based on an automated process.[89] Essentially, it is prohibited to establish methods for deciding exclusively based on an automatic procedure, where such decisions may have an impact on the legal sphere of the affected persons. Article´s 22 provision is quite narrow and does not include preparatory activities taken before a decision-making process, as the creation of the original profile criteria.[90] Profiling, as defined by the GDPR, refers to both the creation and the use of profiles.

As we have already underlined, the safeguard of Article 22 is applied only if the decision is based solely on automated processing. Since "based solely" is not further defined in the regulation, the regulation allows for an interpretation that excludes any human involvement whatsoever. This creates a dangerous loophole, making Article 22(1) inapplicable to many present automated decision-making methods.

Attending the formula "solely based", the law says that this prohibition occurs when the law is taken exclusively on the basis of an automatic procedure. This means, therefore, that if there is any human control over the conclusion or the proposal to conclude that the intelligent machine has arrived, we are no longer in the framework of a purely automated decision. It has been understood that human control exercised over the decision of the intelligent machine must be significant, but unfortunately, if it includes a human action into the chain, then this is enough to circumvent the prohibition.

---

88 Lilian Edwards; Michael Veale, *Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for*. Duke Law and Technology Review, 16 (1) 2017, page 44, Available at: https://scholarship.law.duke.edu/dltr/vol16/iss1/2/, (Last accessed: 05.09.2021).

89 Vítor Fidalgo Palmela; António Menezes Cordeiro, *Direito da proteção de dados : à luz do RGPD e da Lei n.º 58/2019* , Coimbra : Almedina, 2020, page 222.

90 Michael Butterworth, *The ICO and artificial intelligence: The role of fairness in the GDPR framework*, Computer Law & Security Review 34, 2018, pages 257–268.

Therefore, it must be an *effective* control over a mere proposal for a decision that an intelligent machine arrives at.

The issue of *profiling*, which we have already referred to above, is essentially trying to characterize people in terms of data that are known to them for any specific purposes. At the outset the profile is included in the prohibition if it is automatically automated. Still, it has also been said that this depends on the objective. In other words, characterising people according to the data that are known of them is *profiling*. But it is only prohibited if the aim of *profiling* is to try to draw conclusions or make predictions about the individual. If, for example, an enterprise wants to profile its customers only for statistical purposes and have an expanded view of its target audience, but without thereby attempting to draw specific conclusions to a person or another, that will not be a definition of a prohibited profile.[91]

In light of these challenges, we welcome the attempt made by the European Data Protection Board (Former Working Party) to define the scope of solely automated decision-making based on profiling by providing the following clarification:

> 1. "Based solely" on automated processing means that there is no human involvement in the decision process.
> 2. The controller cannot avoid the Article 22 provisions by fabricating human involvement.[92]
> 3. To qualify as human intervention, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the available input and output data.[93]

We agree that a controller should not be able to avoid the Article 22 provisions by fabricating human involvement and that human intervention must involve meaningful oversight. However, we would like to see a more comprehensive explanation on what qualifies as meaningful human intervention, especially in light of complex and opaque forms of advanced processing.

Meaningful human intervention or oversight is challenging to define. On the one hand, human decision-making can be significantly influenced, shaped and prejudiced by profiles that are produced by purely automated means. The propensity for humans to prefer automated system recommendations over conflicting information provided by humans, even if it is accu-

---

[91] Lourenço Noronha dos Santos, *Inteligência Artificial e Direito*, § 12 Inteligência Artificial e Privacidade, Coordination Rocha, Manuel Lopes; Pereira, Rui Soares, Colaboration Ana Coimbra Trigo, Almedina, 2020, pages 153-154.

[92] European Data Protection Board, Former Article 29 Data Protection Working Party, , page 21.

[93] ibid.

rate, is well known in the literature on automation bias.[94] The rapid rollout of AI and automation as protagonists in the future, made us appreciate the risks of letting machines lead human thinking. At the heart of the problem is the fundamental way that AI and automation essentially work as we know by learning from large sets of data. This type of calculation leads to the belief that things will not be drastically different in the future. There's also the possibility that if the training information is inaccurate, the learning will be inaccurate as well.[95]

On the other hand, if the processing is opaque, oversight will be meaningless. This is especially important in the context of advanced processing that relies on computational algorithms, machine-learning and vast volumes of data, as we discussed at the beginning of our analysis. Such processing can be complex and opaque, and as a result, those who base their decisions on them are not necessarily aware of its functions and relative shortcomings. In this case, even if a human being makes the final decision, an automated process has effectively decided for them without the human being having the capacity to meaningfully query that decision.

To qualify as meaningful human intervention, the individuals making such decisions should be able to determine whether the profile that informs their decision is accurate, fair and non-discriminatory. This requires that the individual providing meaningful human oversight has a sufficient level of technical understanding, particularly about the numerous ways in which profiling and automated decision-making can lead to unfairness, inaccuracies. It also requires that the system used to make or inform a decision is sufficiently interpretable, auditable and explainable. Especially in the context of Big Data analytics and Machine-Learning, it is not always feasible to consider all the available input and output data. It is also insufficient to demonstrate meaningful human involvement.

We agree with Veale and Edwards[96] that Data Protection Impact Assessments would be a natural place to assess whether a decision is indeed based on solely automated processing. One way to demonstrate actual oversight would be to document how often a human decisionmaker actually intervenes in decisions and whether their intervention changes the result of the decision.

---

94 Kathleen Mosier; Linda Skitka; Susan Heers; Mark Burdick, *Automation Bias: Decision Making and Performance in High-Tech Cockpits*, The International journal of aviation psychology. 8.(1), 1997, pages 49-50, Available at DOI:10.1207/s15327108ijap0801_3, (Last accessed: 05.09.2021).

95 "What is automation bias and how can you prevent it?", Insights, Bringing Ingenuity to Life, Available at: https://www.paconsulting.com/insights/what-is-automation-bias-how-to-prevent/, (Last accessed: 05.09.2021).

96 Veale, Michael; Edwards, Lilian, *Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling*,Computer Law & Security Review 34(2) 2018, pages 398-404, Available at: DOI: 10.1016/j.clsr.2017.12.002, (Last accessed: 05.09.2021).

4.2. DECISIONS WITH "LEGAL OR SIGNIFICANT EFFECTS" FOR THE DATA SUBJECT

Article 22(3) lists the minimum requirements that have to be met for lawful automated decision-making. There are no ambiguities in the language that would require further interpretation concerning the minimum requirements that must be met by data controllers. As long as these requirements are met, automated decision-making is lawful and in compliance with the GDPR.

The safeguards laid out in Article 22(3) only apply to decisions that are "solely based on automated processing" and produce "legal" or "similarly significant" effects on the data subject. "Legal" and "significant" effects are not defined in the GDPR. A legal effect might be something that adversely impacts an individual's legal rights, or affects his or her legal status. A significant effect is more difficult to explain, but suggests some consequence that is more than trivial and potentially has an unfavourable outcome.[97]

Recital 71[98] of the GDPR provides very limited examples of activities that would have a significant effect. As a result, it is unclear whether the nature of "effects" depends on the subjective perception of the data subject or data controller, or whether some objective standards can be established to determine forms of automated decision-making that inherently produce significant effects. Data processing can significantly affect someone if the effects are more than trivial, meaning that the effects should be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned. At its most extreme, the decision may lead individuals to be excluded or discriminated against as a result of the decisions.[99]

As it stands, the European Data Protection Board has opted for a nuanced subjective interpretation of "significant effect" that runs the risk of placing the burden of proof on the data subject. According to the draft guidance on profiling, "processing that might have little impact on individuals generally may, in fact, have a significant effect on certain groups of society, such as minority groups or vulnerable adults."[100]

This guidance raises several important questions: who defines whether a targeted data subject is vulnerable? An individual with financial difficulties and gambling addiction is clearly vulnerable, but what about women that are

---

97 ICO, Information Commissioner's Office, "Feedback Request — Profiling and automated decision-making.", v1.0, 2017, page 19, Available at: https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf, (Last accessed: 05.09.2021).

98 Recital 71 EU GDPR, Profiling, Available at: https://gdpr-info.eu/recitals/no-71/, (Last accessed: 05.09.2021).

99 European Data Protection Board, Former Article 29 Data Protection Working Party, page 21.

100 ibid.

concerned about their appearance and receive ads for diets and plastic surgery? Arguably, it should be for the controllers to ensure that profiling does not significantly affect individuals according to an objective standard.

Many decisions made today by AI systems fall under the scope of Article 21(1), as AI algorithms are increasingly deployed in recruitment, lending, access to insurance, health services, social security, and education. The use of AI makes it more likely that a decision will be "solely" based on automated processing. This is due to the fact that humans may not have access to all the information that is used by AI systems and may not have the ability to analyse and review how information is used.

It may be impossible, or it may take an excessive effort, to carry out an effective review unless the system has been effectively engineered for transparency, which in some cases may be beyond the state of the art. Thus, especially when a large-scale opaque system is deployed, humans are likely to merely execute the automated suggestions by AI, even when they are formally in charge. Moreover, human intervention may be prevented by the costs-and-incentives structure in place: humans are likely not to substantially review automated decisions, when the cost of engaging in the review – from an individual or an institutional perspective – exceeds the significance of the decision (according to the decision-maker's perspective).[101]

4.3. EXCEPTIONS OF THE GENERAL PROHIBITION OF ARTICLE 22/2

The prohibition on automated decision-making in Article 22(1) operates only under certain conditions. GDPR established three exceptions of the rule of prohibition, allowing controllers to carry out profiling and automated decision-making that have a legal effect, or significantly affect the data subjects in the following cases:

1. where it is necessary for entering into, or performance of a contract between the data subject and a controller;
2. where it is authorised by EU or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
3. where it is based on the data subject's explicit consent.

There are, as a result, several cases where, even if we have an exclusively automated decision, it can be permitted by law. One of the cases is that the possibility of an ex-algorithm remedy for a given decision is legally foreseen. The most typical example is that, currently, with the regulation in the banking

[101] Giovanni Sartor, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, EPRS | European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 641.530 – June 2020, page 60.

sector, banks can establish algorithms to detect the risk of fraud and money laundering. There is a legal provision that expressly allows the use of the automated decision and, therefore, does not pose a challenge.

The second exception is the one where, although there is no legal provision, it is necessary to use the algorithm, an automated decision, for the execution of a contract. Therefore, this must be interpreted in the light of the principle of necessity, which means that it is entitled to use algorithms in this context demonstrating that their use is, among the appropriate means to achieve the end in question, the least onerous of all, that is, that there is no less intrusive means of privacy that guarantees the same objective.[102] We should pay very close attention when we interpret the "necessary" because even if it can be demonstrated that the use of the algorithm would be necessary for the performance of the contract, it does not legitimise the processing when it comes to sensitive data. In other words, in the case of sensitive data, ethnicity, sexual orientation, political convictions, religion, health, even if we can demonstrate that there is a need to use an algorithm for the proper performance of a contract, we will not be able to make use of the automated decision without the consent of the holder.

Therefore, if one of these exceptions applies (entering a contract, authorized by law or, most crucially, based on explicit consent (Article 22(2)), the controller shall adopt measures to safeguard the data subject's legitimate interests, rights, and freedoms and must provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subjects.

a) Consent of data subject

The third source of legitimacy when resorting to automated decisions would be to have the consent of the data subject. Taking a deeper look into the concept of the consent of the data subjects we need to distinguish two phases, the *ex ante* and the *ex post*. Before consenting to automated decision-making, the data subjects need to be given sufficient information to judge whether profiling is safe and will be to their benefit. In addition, data subjects should be notified about the extent to which automated decisions will rely on data that has been derived or predicted through profiling. The EDPB urges data controllers to provide advice on whether "credit scoring methods used are regularly tested to ensure they remain fair, effective and unbiased."[103]

For this to be meaningful, it should include the following main information, for instance, what data will be used as input, what categories of information

---

[102] Lourenço Noronha dos Santos, *Inteligência Artificial e Direito*, § 12 Inteligência Artificial e Privacidade, Coordination Rocha, Manuel Lopes; Pereira, Rui Soares, Collaboration Ana Coimbra Trigo, Almedina, 2020, page 154.

[103] European Data Protection Board, Former Article 29 Data Protection Working Party, page 26.

data controllers intend to derive or predict, how regularly input data are updated, whether the actions of others affect how data subjects are profiled, the presence of algorithms and what kinds of measures the data controller will take to address and eliminate bias, inaccuracies and discrimination. Since misidentification, misclassification and misjudgement are inevitable risks associated with profiling, controllers should also notify the data subject about these risks and their rights to access and rectification.

Inevitably, we should consider that for this consent we always compete with economic factors. Looking into marketing, someone who has consented that their data should be processed automatically for marketing purposes will have done so perfectly freely. But on the other hand, for instance, if someone is looking for life insurance, health insurance, and the following message appears: "There is a series of data that we are going to have to include in the system and will see to be treated automatically", the person knows that if he or she does not give his or her consent, the terms of the insurance contract will be much more costly than otherwise. In this type of situation, it may be relatively illusory that consent given is completely free consent.

After a decision has been made, data subjects need to be able to establish whether profiling has been either unlawful or unfair. For instance, "why did I get this outcome rather than some other outcome?". All of these questions can only be answered through an *ex post* explanation of an individual decision. We would suggest that information about "the logic involved" should include giving data subjects access to the data on which such a decision was based, in combination with information about the way in which it was automatically processed. In addition, Data Protection Authorities (DPAs) should be in a position to audit automated decisions, to test for bias and unlawful discrimination.

Lastly, within this obligation of explanation, there are still some limitations. For example, a company is not obliged to explain thoroughly the algorithmic logic because of the fact that sharing it would constitute the revelation of a trade secret or a full explanation would go to a point in which the intellectual property is underlying. As a result, in cases like this, we agree with Noronha,[104] that what is sought is a balance between being able to go to a point where the holder understands the decision, but always with the protection of the business secrets and intellectual property of the controller.

[104] Lourenço Noronha dos Santos, *Inteligência Artificial e Direito*, § 12 Inteligência Artificial e Privacidade, Coordination Rocha, Manuel Lopes; Pereira, Rui Soares, Collaboration Ana Coimbra Trigo, Almedina, 2020, page 155.

4.4. THE SAFEGUARD MEASURES AGAINST AUTOMATED DECISIONS UNDER ARTICLE 22(3)

In the cases under Article 22(2)(a) and (c), when the automated decision is necessary to contract or explicitly consent, Article 22(3) requires suitable safeguard measures. The data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

Algorithmic auditing, data minimisation, and anonymisation or pseudonymisation, and certification mechanisms are some of the examples. Such measures should ensure that the requirements set forth in Recital 71, concerning acceptability, accuracy and reliability are respected. The controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that those factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised.

Additionally, the data controller shall secure the personal data so as to consider (in a manner that considers) the potential risks involved for the interests and rights of the data subject and to prevent, *inter alia,* any discriminatory effects on natural persons regarding racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect.

The input data must be shown to not be "inaccurate or irrelevant, or taken out of context," and to not violate "the reasonable expectations of the data subjects", in relation to the purpose for which the data was collected.[105] In approaches based on machine-learning, this should apply not only to the data concerning the person involved in a particular decision, but also to the data in a training set, where the biases built into the training set may affect the learned algorithmic model, and hence the accuracy of the system's inferences.

Other measures pertain to the interaction with the data subjects, such as the right to obtain human intervention and the right to challenge a decision, one that we will analyse in the next chapter. As an example, a link could be provided to "an appeal process the moment when the automated decision is delivered to the data subject, with agreed time scales for the review and a named contact point for any queries"[106]. An appeal process is most significant with regard to AI applications, and especially when these applications

---

[105] Sandra Wachter; Brent Mittelstdt, "A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI", April 2019, page 96, Available at: https://www.researchgate.net/publication/327872087_A_RIGHT_TO_REASONABLE_INFERENCES_RE-THINKING_DATA_PROTECTION_LAW_IN_THE_AGE_OF_BIG_DATA_AND_AI, (Last accessed: 10.09.2021) .

[106] Article 29 Data Protection Working Party, page 32.

are opaque and for instance, unable to provide human-understandable explanations and justifications.

4.5. A PROHIBITION OR A RIGHT TO OBJECT?

Unquestionably, Article 22 of the GDPR is a welcome development. The doctrine has raised doubts concerning its legal nature. The legal order and the writing of the article lead us to classify it alongside other rights of the data subject. However, considering the content of the rule, it seems to establish, in the first place, additional legal requirements to those that are broadly provided in the GDPR,[107] based on the general prohibition of automated decisions.[108]

This is a significant right that addresses the growing reliance on automated decisions. However, there is a vigorous debate in the academic literature on whether such a right to explanation should indeed be given to the data subject. Goodman and Flaxman sparked the debate by inferring such a right from the requirement to give the data subject meaningful information about the logic involved derived from Articles 13 and 14.[109] Articles 13 and 14 state that, when profiling takes place, a data subject has the right to "meaningful information about the logic involved." This requirement prompts the question: what does it mean, and what is required, to explain an algorithm's decision?

There are numerous issues with the wording of Article 22 that can lead to asymmetrical interpretations and enforcement gaps. A prohibition or right to object? According to Wachter et al. GDPR only requires an *ex ante* explanation of how the system functions and not *ex post* explanation of the reasons behind the decision and why this decision was made.[110] As Hildebrandt writes, "correlations stand for a probability that things will turn out the same in the future. What they do not reveal is why this should be the case".[111] On the other hand, Edwards and Veale accept the possibility of the right to explanation, but point out practical difficulties of its exercise from the per-

---

[107] Buchner, *Anotação ao artigo 22.º do RGPD* in Külhing/Buchner, Rn. 12.

[108] Vítor Fidalgo Palmela; António Menezes Cordeiro, *Direito da proteção de dados : à luz do RGPD e da Lei n.º 58/2019*, Coimbra : Almedina, 2020, page 223.

[109] Bryce Goodman; Seth Faxman, "European Union regulations on algorithmic decision-making and a 'right to explanation'", page 6, Available at: https://arxiv.org/pdf/1606.08813v3.pdf, (Last accessed: 05.09.2021).

[110] Sandra Wachter; Brent Mittelstadt; Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", International Data Privacy Law, 2017, Vol. 7, No. 2. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469, (Last accessed: 05.09.2021).

[111] Mireille Hildebrandt, *Defining profiling: a new type of knowledge?*, Springer, 2008, Springer, page 1745.

spective of Machine-Learning algorithms.[112] Lastly, Mendoza and Bygrave equally argued in favour of the right to explanation.[113]

Felletti claims that the specific measures of the provision of Article 22, are appropriate and require human intervention, "someone who has the necessary authority, ability, and competence to modify or revise the decision disputed by the user." She also addresses the idea that in striving to provide transparency, explanations of technical subject matter such as AI "may not be sufficient if the information received is not comprehensible to the recipient." Lastly, Falletti asserts that instead of explaining how an algorithm works, providing comprehensible information and describing the relative emphasis placed on different information would be appropriate.[114]

In the light of that, the provisions of the GDPR, more precisely, Article 22, read in the light of Recital 71, in combination with Articles 13(2)(f), 14(2)(g) and 15(1)(h) GDPR, should be interpreted so as to give the data subject the right to an *ex post* explanation of the automated decision. Such methodological grouping of different data protection provisions in order to create a certain right of the data subject is not unusual in the case law of the CoJ. For example, in Google Spain, the Court relied on the combination of the right of access and the right to object from Directive 95/46[115] in order to judicially construct the right to erasure, widely described as "the right to be forgotten".[116]

The wording of the "right not to be subject to automated decision-making" of Article 22 GDPR can be interpreted as either a prohibition or a right to object. Resolving this ambiguity is critical, since it greatly affects how strongly data subjects are protected. If interpreted as a right to object, data subjects could object to being subject to automated decision-making, unless the conditions in Article 22(2)(a)-(c) apply. If interpreted as a prohibition, data controllers would not be allowed to engage in automated individual decision-making, unless the conditions in Article 22(2)(a)-(c) are met the

---

112 Lilian Edwards; Michael Veale, "Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for.", Duke Law and Technology Review, 16 (1) 2017, Available at : https://scholarship.law.duke.edu/dltr/vol16/iss1/2/, (Last accessed: 05.09.2021).

113 Isak Mendoza; Lee Andrew Bygrave, "The Right not to be Subject to Automated Decisions based on Profiling", University of Oslo Faculty of Law Legal Studies Research Paper Series No. 20/2017, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855, (Last accessed: 05.09.2021).

114 James Alford; Milad Emamian; Emily Galik; Allie Gottlieb; Lila Sevener, "GDPR and Artificial Intelligence", Saturday Seminar, Technology, The Regulatory Review, May 9, 2020, Available at: https://www.theregreview.org/2020/05/09/saturday-seminar-gdpr-artificial-intelligence/, (Last accessed: 05.09.2021) .

115 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 OJ L 281/31.

116 The CoJ relied on Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46; Case C-131/12 Google Spain and Google ECLI:EU:C:2014:317.

conditions would have to be met. So, before entering into or performing a contract, authorised by law, or explicit consent.

4.6 AUTOMATED DECISION-MAKING AND SENSITIVE DATA UNDER ARTICLE 22(4)

Article 22 is designed with an admirable objective at its core, to prevent any unfair bias or discrimination from entering into a decision. Profiling, as part of AI decision-making, could result in repercussions when collecting and processing sensitive data such as race, age, health information, religious or political beliefs, shopping behaviour and income. If misused, the darkest side of automated profiling means that more vulnerable segments of society will bear the brunt of any negative outcomes. However, one of the major criticisms about the game-changing regulation is its ambiguous language that could result in serious misinterpretation.

Article 22(4) is explicitly introducing a prohibition, limited by an exception, to ground automated decisions on "sensitive data", the special categories set out in Article 9(1).[117] The exception concerns the cases in which the data subject has given explicit consent. The role of the data subject's consent needs to be clarified since consent does not exclude that the method used for the decision is unacceptable (as when it is discriminatory).

As previously stated, AI challenges the restriction of sensitive data processing. To begin with, sensitive data can be deduced probabilistically from non-sensitive data. For example, a data subject's sexual orientation can be deduced from their Internet activity, likes, or even facial characteristics. Under this scenario, the inference of sensitive data should be regarded as a processing of sensitive data, and therefore would have to be considered unlawful unless the conditions under Article 9 are met. Other example: the place of residence can be used as a proxy for ethnicity.[118] [119] In this case, unlawful discrimination may take place.

In the sense of the enhanced protection that GDPR has given to sensitive data, Article 22(4) came to re-enforce this protection by limiting the scope of

---

[117] Article 9(1)- Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

[118] Inês Silva Costa, *A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas*, Revista Electrónica De Direito, No 1, (VOL. 24) February 2021, pages 47 Available at: https://cije.up.pt/pt/red/edicoes-anteriores/2021-nordm-1/a-protecao-da-pessoa-na-era-dos-big-data-a-opacidade-do-algoritmo-e-as-decisoes-automatizadas/, (Last accessed: 05.09.2021).

[119] See more Joshua A. Kroll; Joana Huey; Solon Barocas; Edward W. Felten; ReidenJoel R. berg,; David G. Robinson; Harlan Yu, "Accountable Algorithms", , in University of Pennsylvania Law Review, vol. 165, 2017, pages 680-681, Available at: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9570&context=penn_law_review, (Last accessed: 05.09.2021).

the exception provided in paragraph 2.[120] As a result, even though the system does not infer sensitive data, non-sensitive data can act as proxies for sensitive data associated with them.

5. ARTIFICIAL INTELLIGENCE AND PERSONAL DATA: RISKS AND OPPORTUNITIES

Amid the cacophony of concerns over AI taking over jobs, the potential for AI to do good can be overlooked. As we underlined at the very beginning of our analysis, technology leaders such as Microsoft, IBM and Google have entire sections of their business focused on the topic and dedicate resources to build AI solutions and to support such developers.[121] In the fight to solve extraordinarily difficult challenges, we humans must use all the help they can get. There are many powerful examples of AI usage for good as it is applied to some of the toughest challenges facing society today.[122]

Theoretically, automation and AI should free humans from dangerous or boring tasks so they can take on more intellectually stimulating assignments, making companies more productive and raising workers' wages. In the past, technology was implemented in stages, giving employees time to transition and adapt to new roles. Those who lost jobs could seek retraining, perhaps using severance pay or unemployment benefits to find work in another field. Nowadays, the change was abrupt as employers, worried about COVID-19 or under sudden lockdown orders, rushed to replace workers with machines or software. There was no time to retrain. Companies that were concerned about their bottom line have cut workers loose instead, and these workers were left on their own to find ways of mastering new skills.

There are numerous difficulties and challenges that need to be solved today to enable a better tomorrow for our planet, cultures and society. When humans collaborate with AI, solutions that would not have been considered otherwise can be developed and vetted at a pace that would not be possible if only humans were tasked with the assignment. AI provides innovative ways of solving extremely challenging problems while at the same time providing ways of significantly improving life. As we have already covered above, there are such multiple legal implications in the use of AI algorithms. Reis lists several

---

120 Vítor Fidalgo Palmela; António Menezes Cordeiro, *Direito da proteção de dados: à luz do RGPD e da Lei n.º 58/2019*, Coimbra : Almedina, 2020, page 226-227.

121 See more in Samuels Alana, "Millions of Americans Have Lost Jobs in the Pandemic—And Robots and AI Are Replacing Them Faster Than Ever", Times Magazine, August 2020, Available at: https://time.com/5876604/machines-jobs-coronavirus/, (Last accessed: 05.09.2021).

122 See more Bernard Marr, "8 Powerful Examples Of AI For Good", Forbes, February 2020 Available at: https://www.forbes.com/sites/bernardmarr/2020/02/10/8-powerful-examples-of-ai-for-good/?sh=1dcd13f0d18a, (Last accessed: 05.09.2021).

areas such as surveillance systems, biometric identification systems, using advanced AI algorithms, robots that rule almost one third of the internet traffic among many others. Systems of AI that neither Asimov could have made.[123]

It is necessary to say that the GDPR, despite the fact that it came to bring a lot of news and is coming to bring a lot of solutions to problems that the intelligence was and is putting in, it does not solve everything. Noronha refers to the existence of institutions that mention the lack of regulation in cases where the violation does not concern personal data. For example, a lip reading system that is applicable in a public space. Possibly it might not have been in violation of any personal data, but there could still be an intrusion of the sphere of privacy.[124]

To what relates to our analysis, the growth of AI is being affected by the way governments regulate it and the large volumes of digitally stored data on which AI depends. The GDPR has been described as "the toughest privacy and security law in the world," and some commentators assert that various provisions of the Regulation are affecting the development of AI within countries in Europe, such as startups or even technology firms. Most specifically, the provision of Article 22. It is believed that this provision could lead AI companies to limit activities such as offering customers loans or to implement an additional and expensive human review of AI-powered decisions.[125] Kalliopi Spyridaki argues that even though the GDPR might limit or complicate how data are being handled and used by AI, the Regulation can also help create the trust that is necessary for AI acceptance by consumers and governments.

5.1. ETHICAL QUESTIONS AND CHALLENGES UPON AI AND AUTOMATED DECISION-MAKING

Concerning the existing dangers of the ethical questions around AI, Walker describes "Ethical AI" as a red herring.[126] In advanced software algorithms there are almost always many operational biases. This happens because humans are inherently biased while writing softwares directly or indirectly and because the data that are used to develop the algorithmic processes are

123 Paulo Victor Alfeo Reis, *Algoritmos e o direito*, São Paulo: Almedina, 2020, page 178.

124 Lourenço Noronha dos Santos, *Inteligência Artificial e Direito*, § 12 Inteligência Artificial e Privacidade, Coordination Rocha, Manuel Lopes; Pereira, Rui Soares, Collaboration Ana Coimbra Trigo, Almedina, 2020, pages 156-157.

125 James Alford; Milad Emamian; Emily Galik; Allie Gottlieb; Lila Sevener, "GDPR and Artificial Intelligence", Saturday Seminar, Technology, The Regulatory Review, May 9, 2020, Available at: https://www.theregreview.org/2020/05/09/saturday-seminar-gdpr-artificial-intelligence/, (Last accessed: 05.09.2021).

126 Joshua Walker, *IS "ETHICAL AI" A RED HERRING?*, 36 Santa Clara High Tech. L.J. 445, May 2020, page 445, Available at: https://digitalcommons.law.scu.edu/chtlj/vol36/iss4/1(Last accessed: 07.09.2021).

also derived, directly or indirectly from said biased humans.[127] [128] As Walker says, "*both the creative matrix and the authors, the data and the humans, necessarily and naturally introduce bias into AI*".

The debate around Ethical AI is much needed. Concerning the textual problematic, the word "ethical" is as much subjective as the word "moral". The term itself seems to be rather an oxymoron. Ethical standards can, in theory, be effectively applied to AI modalities, thus making such AI, together with such exogenous controls, "ethical."[129] The term Ethical AI, is nevertheless, ambiguous because it may imply that for instance an autonomous piece of software, a robot, is fundamentally ethical and consciously applying and developing a moral sense like a human being does.

What deserves our attention is not the textual part of the problem but the operational consequences that flow therefrom. Ethical codes might have serious consequences, but not of a legal binding nature. There is a question lying around the debate of the existence of an Ethical AI. *What is the objective of an AI ethics movement with no objective object?* This movement has been criticised as designed to deflate the fear and doubts connected to advanced software experimentations. The new technologies are applied and in our point of view, should be accompanied by law. The complexity of AI and the issues that derive from its applications make the creation of a new legal framework and legal AI a very difficult task.

Relating to the above debate, the European Commission's legislative proposal for an "Artificial Intelligence Act"[130] is the first initiative worldwide that provides a legal framework for AI in compliance with the European values and legal principles. The European Parliament Resolution on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies[131] specifically recommends to the Commission to propose legislative action

---

127 See more Joshua A. Kroll; Joana Huey; Solon Barocas; Edward W. Felten; ReidenJoel R. berg,; David G. Robinson; Harlan Yu, "Accountable Algorithms", , in University of Pennsylvania Law Review, vol. 165, 2017, page 681, Available at: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9570&context=penn_law_review, (Last accessed: 05.09.2021).

128 Inês Silva Costa, *A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas*, Revista Electrónica De Direito, No 1, (VOL. 24) February 2021, pages 47-48, Available at: https://cije.up.pt/pt/red/edicoes-anteriores/2021-nord-m-1/a-protecao-da-pessoa-na-era-dos-big-data-a-opacidade-do-algoritmo-e-as-decisoes-automatizadas/, (Last accessed: 05.09.2021).

129 Joshua Walker, *IS "ETHICAL AI" A RED..*, page 445.

130 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts', European Commission, COM(2021) 206 final, Brussels, April 2021, Available at: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2021)206&lang=en, (Last accessed: 05.09.2021).

131 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html, (Last accessed: 05.09.2021).

to harness the opportunities and benefits of AI, but also to ensure the protection of ethical principles. The main objectives of the proposed regulatory framework are the following:

- ensure that AI systems placed and used on the Union market are safe and respect existing law on fundamental rights and Union values;
- ensure legal certainty to facilitate investment and innovation in AI;
- enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
- facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.[132]

The aim of the proposal and the mechanisms it encompasses is the development of an ecosystem of trust through the establishment of a human-centric legal framework for trustworthy AI. Only on the first page of the Memorandum, the word trust appears five times, whereas the actual text of the proposal refers at least ten times to the idea of trust, mainly in recitals.[133] This "importance of creating the trust that will allow the digital economy to develop across the internal market" is also repeated in Recital 7 of the GDPR. The extensive AI Act addresses the risks stemming from the various uses of AI systems and aims to promote innovation in the field of AI. MacCarthy and Propp[134] have called the proposed regulation "a comprehensive and thoughtful start to the legislative process in Europe [that] might prove to be the basis for trans-Atlantic cooperation".[135] The European Commission chose to define the AI systems and not the AI *per se*.[136]

The GDPR model is visible in the provisions of the draft AI Act, structurally and a case-specific one. From a structural perspective, the GDPR effect is best seen in the suggested AI supervision and enforcement model. Essentially, the draft AI Act replicates the GDPR model of establishing supervisory authorities

---

132 Explanatory Memorandum, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts'., European Commission, COM(2021) 206 final, Brussels, April 2021, page 1 Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206, (Last accessed: 05.09.2021).

133 Explanatory Memorandum, ibidem, page 1.

134 Mark MacCarthy; Kenneth Propp, "Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation", Lawfare Institute, Brookings, Artificial Intelligence, April 2021 https://www.lawfareblog.com/machines-learn-brussels-writes-rules-eus-new-ai-regulation, (Last accessed: 05.09.2021).

135 Eve Gaumond, "Artificial Intelligence Act: What Is the European Approach for AI?", Lawfare Institute, Brookings, Artificial Intelligence, June 2021 Available at: https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai, (Last accessed: 05.09.2021).

136 "[A]rtificial intelligence system" (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with[.].

at the national level (Art 3(42) and 59 of the draft AI Act), that are to be coordinated at the EU level by a Board. From a case-specific perspective, provisions in the draft AI Act directly refer to GDPR or are directly affected by it.

The scope of AI regulation is much wider and aims to protect both the individuals and to enhance the development of AI. The issue is that the AI regulation is not connected with a specific activity or field but the AI in the spectrum of human life in general. Any attempt to create a catalogue of AI and its whole scope will be unsuccessful, as it is a very ambitious task.[137]

Papakonstantinou and De Hert refer to "EU law brutality", as the tendency of the European legislator to introduce new constructions and legal mechanisms to support its law-making options in what could be described as a brutal manner. This means that Member State particularities, either legal or any other kind, are in one way or another "glossed over". Without a doubt, the supremacy of EU law is recognised. However, nowadays' technology permeates human lives. There is practically no field of human activity not affected by it. Brownsword identifies that the EU, either by design or by sheer luck, happened to be the one indisputably authorized to regulate digital life, perhaps under a regulatory-instrumentalist mind-set.[138]

5.2. THE NEED OF ALGORITHMIC TRANSPARENCY

We have already seen numerous obstacles and difficulties around the issue of attempting to provide meaningful explanation on an algorithmic schema. If providing meaningful explanation about the logic of a machine-learning algorithm has proven so hard, how sure are we that this is actually an effective remedy towards transparency?[139] Transparency of automated decision making is regarded as a panacea against opaque computing systems. We should underline the fact that complex algorithms which dominate our lives, such as Facebook, Google, YouTube are proprietary shielded as trade secrets, only a vast minority of algorithms are open source.

Regarding trade secrets in general, in the Microsoft case, the CJEU held that a refusal by Microsoft to share interoperability information with a competitor constituted a breach of Article 102 TFEU. Recognising the value of Microsoft's trade secrets, the Court relied on the "exceptional circumstances" doctrine developed in the Magill and IMS Health cases previously, and

---

[137] Vagelis Papakonstantinou; Paul De Hert, "EU law making in the Artificial Intelligent Age: Actification, GDPR mimesis, and regulatory brutality", July 2021, Available at: https://europeanlawblog.eu/2021/07/08/eu-lawmaking-in-the-artificial-intelligent-age-act-ification-gdpr-mimesis-and-regulatory-brutality/, (Last accessed: 05.09.2021).

[138] Roger Brownsword, *Law, Technology and Society. Reimagining the Regulatory Environment.* Routledge, 1st Edition, February 2019, page 194.

[139] Lilian Edwards; Michael Veale, "Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for.", Duke Law and Technology Review, 16 (1) 2017, page 65, Available at : https://scholarship.law.duke.edu/dltr/vol16/iss1/2, (Last accessed: 05.09.2021).

re-established that "the mere fact of holding intellectual property rights could not in itself constitute objective justification for the refusal", otherwise "the raison d'être of the exception which that case-law thus recognises in favour of free competition" would be defeated.

As to algorithms specifically, in the Google Shopping case,[140] the European Commission found that Google had abused its dominant position by demoting rival comparison shopping services in its search results, and thus violated Article 102 TFEU. Although trade secrets remained protected from the public and competitors, Google had to disclose Page Rank parameters to the Commission as the administrative authority for the performance of its investigative duties.

Whilst the GDPR does not contain a separate article dedicated to the interplay with trade secrets, Recital 4 mentions the "freedom to conduct a business". Recital 63 is more specific to the subject, stating that data subject's right of direct access to personal data should not adversely affect, inter alia, trade secrets. As far as it concerns the data subjects' right to explanation, it is epitomised as we have already covered above by Article 22 in conjunction with Article 15 of GDPR and Recital 71.

Ananny and Crawford[141] recall several ways in which transparency used "as a method to see, understand and govern complex systems", both in the past, and now in the time of algorithmic Machine-Learning and Big Data systems, is not only limited but at times misleading and unhelpful. Inter alia, they note that transparency can support "neoliberal models of agency," placing a tremendous burden on individuals both to seek out information about a system, interpret it, and determine its significance, only then to find out they have little power to change things anyway, being "disconnected from power". In the past, liberal democracy has taught us "the feeling that seeing something may lead to control over it". However, in its search for a technical solution, dependence on transparency may occlude the true problems which rest in societal power relations and institutions as much as in the software tools used.[142]

Algorithmic decisions are likely to become more and more reliable for a range of decisions with potentially important repercussions for those individuals that are affected by them. Understanding how people evaluate the

---

140 Case AT.39740 — Google Search (Shopping), 27 June 2017, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1516198535804&uri=CELEX:52018XC0112(01), (Last accessed: 05.09.2021).

141 Mike Annany; Kate Crawford, *Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability,* New Media & Society 1, December 2016, page 5, Available at: https://doi.org/10.1177/1461444816676645, (Last accessed: 05/09/2021).

142 Lilian Edwards; Michael Veale, "Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for.", Duke Law and Technology Review, 16 (1) 2017, page 66 Available at : https://scholarship.law.duke.edu/dltr/vol16/iss1/2, (Last accessed: 05/09/2021).

fairness of the automated-decisions as well as how explanations can help, is therefore of increasing significance. As Woodruff underlined, explanations are a potential mechanism to ameliorate the concerns raised against the deployment of AI systems.[143] Explanations can provide plausibly transparency, allowing individuals to detect possible errors and laying the groundwork for appeals to change the decisions.

5.3. DATA PROTECTION IMPACT ASSESSMENT AND AI

On the virtue of AI and Big Data, GDPR has introduced a number of new provisions which do not confer individual rights but attempt to create an environment in which non-toxic automated systems can be created in the future. These ideas derive from a long evolution of so-called Privacy by Design engineering as a way to build privacy-aware or privacy-friendly systems, starting from the beginning of the process of design. They recognize that a regulator cannot do a thorough control, unless the controllers themselves are involved in the design of less privacy-invasive systems.

Article 25 of GDPR and Recital 78[144] states that controllers must, at the time systems are developed as well as at the time of actual processing, implement "appropriate technical and organisational measures" to protect the rights of the data subjects. In particular, "data protection by design" is required so that only personal data necessary for processing are gathered. Suggestions for Privacy by Design include pseudonymisation and data minimisation. In addition, Article 35 of GDPR introduces the existence of the Data Protection Assessment (DPIA) when a type of processing using new technologies is "likely to result in a high risk" to the rights of data subjects. Moreover, Article 6 states that every public authority and every large-scale private sector controller and any controller processing special categories of sensitive data must appoint a Data Protection Officer (DPO) in the case of sensitive data control.

Therefore, Article 35(3) obliges the data controllers to carry out a DPIA for high risky processing, in particular whenever AI and other new technologies are used to profile or extensively evaluate citizens with legal or similarly significant effects, and public accessible data is systematically monitored, or sensitive data are processed at large scale. Former Article 29 Working Party[145] has further stated that the processing is high-risky, and

---

[143] Allison Woodruff; et al.,""A cold, technical decision-maker": Can AI provide explainability, negotiability, and humanity?" 1, 1, Association for Computing Machinery, December 2020, page 10, Available at: https://arxiv.org/pdf/2012.00874.pdf, (Last accessed: 05.09.2021).

[144] Recital 78, Available at: https://www.privacy-regulation.eu/en/recital-78-GDPR.htm, (Last accessed: 05.09.2021).

[145] Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 4 October 2017, 17/EN WP 248.

controllers must carry out a DPIA, if two or more conditions included in a long list are met, however subjecting to prior assessment practically every AI system intended to process personal data. As we have already referred in our fourth chapter, the high-risk of algorithmic bias, the assessment of the specific risk of discrimination should be an obligatory step in the design and use of every AI system as part of solely automated or partially automated decision-making process(es).

More specifically, it may be possible to link observable behaviour and known features of individuals, their online activity, purchases, likes, to non-observable sensitive data on them such as their psychological attitudes, their health condition, their sexual orientation, or their political preferences. Such inferences may expose the concerned individuals to discrimination or manipulation. However, we cannot forget that algorithmic decisions may also be mistaken or discriminatory, reproducing human biases and introducing new ones. Even when automated assessments of individuals are fair and accurate, they are not unproblematic. They may negatively affect the individuals concerned, who are subject to pervasive surveillance, persistent evaluation, insistent influence, and possible manipulation.[146]

According to the ICO framework for auditing AI and its key considerations, DPIAs should provide a systematic description of the processing activity, including data flows and the stages when AI processes and automated decisions may produce effects on individuals. Organisation should seek and document the views of individuals on the intended processing operation during a DPIA. It is essential to be able to explain and describe the process in a way that is user friendly. But as we have mentioned, describing a complex AI system can be a very challenging task. ICO proposes that maintaining two versions of assessments would be the appropriate solution. The first presenting a thorough technical description for specialist audiences. The second containing a more high-level description of the processing and explaining the logic of how the personal data inputs relate to the outputs affecting individuals.[147]

Necessity and proportionality should be assessed. The deployment of an AI system to process personal data needs to be driven by the proven ability of that system to fulfil a specific and legitimate purpose and not by the availability of the technology. An organisation can evidence that these purposes could not be achieved in another reasonable way, by assessing necessity

---

146 Giovanni Sartor, "The impact of the General Data Protection Regulation (GDPR) on artificial intelligence", Scientific ForesightUnit (STOA), Panel for the Future of Science and Technology, June 2020, page 1, Available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530, (Last accessed: 05.09.2021).

147 UK Information Commissioner's Office: Data Protection Impact Assessments and AI, 23 October 2019, Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/, (Last accessed: 05.09.2021).

in a DPIA. At the same time, proportionality should also be assessed. It is important to balance the interests of the organisation against the rights and freedoms of the individuals. Organisations need to think about any detriment to data subjects that could follow from bias or inaccuracy in the algorithms and data sets being used.

6. EPILOGUE

Concluding our analysis, framing and regulating AI has proven a very difficult task. The implications of AI on privacy and data protection raise doubts considering the adequacy of GDPR to respond to the new challenges. GDPR regulates AI when personal data is being processed. As we underlined throughout our analysis, AI is advancing more rapidly than the process of finding answers to ethical and legal questions. Bayamlıoğlu, in her analysis related to the automated decisions in the GDPR, points out Bygrave's critique upon the former Article 15 of DPD, currently 22 of GDPR, and the accuracy of his phrase: "all dressed up but nowhere to go"?[148] [149]

GDPR is the first piece of legislation that tried to regulate AI. Since its full effect in 2018, the law has significantly shaped how data protection is conducted around the world. The recent proposal to a new AI Act, seems to want to replicate the same kind of regulatory influence achieved with the GDPR. The main question raised by this initiative is if it makes sense to regulate a situation prematurely, before the main challenges appear, or when the challenges appear then it would be too late to regulate. On the other hand, the AI Act should complete the GDPR and the two documents should not overlap each other.

In addition, we always need to carefully foresee the equilibrium between innovative AI systems and the protection of the fundamental rights and personality rights of the individuals. This task is very delicate and very challenging. In the middle of the debates and the fears against AI's automated systems, we should not forget that AI systems are taking a protagonistic place in our everyday lives and facilitate it in many ways. As AI, Big Data and Machine-Learning evolve, regulators seek to protect the public and the fundamental rights of the individuals without stifling innovation. Because these technologies rely on ever-growing volumes of data, laws such as the GDPR could limit AI development. However, as Niemitz highlights, not binding AI

[148] Emre Bayamlıoğlu, "Transparency of Automated Decisions in the GDPR: An Attempt for Systemisation", January 2018, page 50, Available at SSRN: https://ssrn.com/abstract=3097653, (Last accessed: 05.09.2021).

[149] Lee A Bygrave, *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, Computer Law & Security Review, Volume 17, Issue 1, 1 January 2001, pages 17-24.

systems to the basic constitutional principles would lead us to a "widespread culture of disregard of the law and put democracy in danger".[150]

7. BIBLIOGRAPHY

Alana, Samuels, "Millions of Americans Have Lost Jobs in the Pandemic—And Robots and AI Are Replacing Them Faster Than Ever", Times Magazine, August 2020, Available at: https://time.com/5876604/machines-jobs-coronavirus/, (Last accessed: 05.09.2021)

Alford, James; Emamian, Milad; Galik, Emily, Gottlieb; Allie, Sevener, Lila, "GDPR and Artificial Intelligence", Saturday Seminar, Technology, The Regulatory Review, May 9, 2020, Available at: https://www.theregreview.org/2020/05/09/saturday-seminar-gdpr-artificial-intelligence/, (Last accessed: 05.09.2021)

Algorithms, Computer Science Wiki, https://computersciencewiki.org/index.php/Algorithms, (Last accessed: 05.09.2021)

Annany, Mike; Crawford, Kate, *Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability,* New Media & Society 1, December 2016, Available at: https://doi.org/10.1177/1461444816676645, (Last accessed: 05/09/2021).

Article 29 Working Party Opinion 4/2007 on the concept of personal data, Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf,(Last accessed: 05.09.2021)

Article 29 Working Party, Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 4 October 2017, 17/EN WP 248

Article 29 Working Party, Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, Available at: https://www.dataprotection.ro/servlet/ViewDocument?id=1088, (Last accessed: 05.09.2021)

Big Data definition, Gartner Glossary, Information Technology Glossary, Available at: https://www.gartner.com/en/information-technology/glossary/big-data, (Last accessed: 05.09.2021)

Bostrom, Nick; Yudkowsky, Eliezer, "The Ethics of Artificial Intelligence.", Cambridge Handbook of Artificial Intelligence, edited by Keith Frankish and William Ramsey. Machine Intelligence Research Institute, New York: Cambridge University Press, Available at: https://intelligence.org/files/EthicsofAI.pdf, (Last accessed: 05.09.2021)

Boucher, Philip, *Artificial intelligence: How does it work, why does it matter, and what can we do about it?*, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), June 2020, Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf, (Last accessed: 05.09.2021)

[150] Paul Niemitz, "Constitutional democracy and technology in the age of artificial intelligence", The Royal Society, October 2018, Available at: https://royalsocietypublishing.org/doi/full/10.1098/rsta.2018.0089#FN2, (Last accessed: 05.09.2021).

Brkan, Maja, *Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond*, International Journal of Law and Information Technology, January 2019, page 91-121, Available at DOI: 10.1093/ijlit/eay017, (Last accessed: 05.09.2021)

Brownsword, Roger, *Law, Technology and Society. Reimagining the Regulatory Environment.* Routledge, 1st Edition, February 2019

Buchner, *Anotação ao artigo 22.º do RGPD* in Külhing/Buchner, Rn. 12

Burri, Mira and Schär, Rahel, The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. Journal of Information Policy, Vol. 6, June 2016, pages 479-511, Available at SSRN: https://ssrn.com/abstract=2792222 or http://dx.doi.org/10.2139/ssrn.2792222, (Last accessed: 05.09.2021)

Butterworth Michael, *The ICO and artificial intelligence: The role of fairness in the GDPR framework*, Computer Law & Security Review 34, 2018, pages 257-268

Bygrave, Lee A, *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, Computer Law & Security Review, Volume 17, Issue 1, January 2001, pages 17-24

Campos, Diogo Leite. Nós – Estudos sobre o Direito das Pessoas. Coimbra: Almedina, 2004.

Canotilho, J.J. Gomes; Moreira, Vital, *Constituição da República Portuguesa anotada*, vol. I. 4.ª ed. rev. Coimbra: Coimbra editora 2014

Carvalho, Orlando, *Teoria Geral do Direito Civil*, Coimbra Editora, 2012

Copeland, Jake, "What is AI?", Alanturing.net., May 2000, Available at: http://www.alanturing.net/turing_archive/pages/reference%20articles/what%20is%20ai.html, (Last accessed: 05.09.2021)

Cordeiro, António Menezes, *Direito da proteção de dados : à luz do RGPD e da Lei n.º 58/2019* , Coimbra : Almedina, 2020

Cordeiro, António Menezes, *Tratado de Direito Civil,* Vol. IV, 5ª ed., Coimbra: Almedina, 2019

Costa, Inês Silva, *A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas*, Revista Electrónica De Direito, No 1, (VOL. 24) February 2021, pages 34 — 82 Available at: https://cije.up.pt/pt/red/edicoes-anteriores/2021-nordm-1/a-protecao-da-pessoa-na-era-dos-big-data--a-opacidade-do-algoritmo-e-as-decisoes-automatizadas/, (Last accessed: 05.09.2021)

Criado, Natalia; Such, Jose M., "Digital discrimination", Algorithmic Regulation, Oxford University Press, 2019, Available at: https://www.researchgate.net/publication/336792693_Digital_Discrimination, (Last accessed: 05.09.2021)

Cruz, Bruno Fernando dos Santos, *Smart Cars: desafios jurídicos na era da inteligência artificial*, Master's Thesis, Faculty of Law, University of Porto, 21 December 2020

Datatilsynet, "Artificial Intelligence and Privacy – Report", The Norwegian Data Protection Agency, January 2018, Available at: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf, (Last accessed: 05.09.2021)

Dwork, Cynthia; Naor†, Moni, *On the Difficulties of Disclosure Prevention in Statistical Databases or The Case for Differential Privacy*, Journal of Privacy and Confidentiality, 2, Number 1, 2010

Edwards, Lilian; Veale, Michael, "Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for.", Duke Law and Technology Review, 16 (1) 2017, Available at : https://scholarship.law.duke.edu/dltr/vol16/iss1/2, (Last accessed: 05.09.2021)

Ethics guidelines for trustworthy AI, Report/Study, Shaping Europe's digital future, April 2019, Available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai, (Last accessed: 05.09.2021)

European Commission (2018b). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions — Coordinated Plan on Artificial Intelligence (COM(2018) 795 final). Available at: https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence, (Last accessed: 05.09.2021)

European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems, European Union, Brussels 2018, Available at: https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf, (Last accessed: 05.09.2021)

European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html, (Last accessed: 05.09.2021)

European Parliament, "What is artificial intelligence and how is it used?", Article, European Parliament, 20200827STO85804, October 2020, Available here: https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used, (Last accessed: 06.09.2021)

Explanatory Memorandum, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts'., European Commission, COM(2021) 206 final, Brussels, April 2021, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206, (Last accessed: 05.09.2021)

Félix da Costa, Tiago; Alfredo Afonso, João, "Portugal-National GDPR Implementation Overview", May 2020, Available at: https://www.dataguidance.com/notes/portugal-national-gdpr-implementation-overview, (Last accessed: 05.09.2021)

Floridi, Luciano, "Big Data and their epistemological challenge." Philosophy and Technology 25(4) 2012, pages 435-437, Available at DOI 10.1007/s13347-012-0093-4, (Last accessed: 05.09.2021)

Gaumond, Eve, "Artificial Intelligence Act: What Is the European Approach for AI?", Lawfare Institute, Brookings, Artificial Intelligence, June 2021 Available at: https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai, (Last accessed: 05.09.2021)

Gonçalves, Diogo Costa, Pessoa e Direitos de Personalidade – Fundamentação Ontológica da Tutela. Coimbra: Almedina, 2008

González, José A.R.L, *Responsabilidade por danos e Inteligência Artificial (IA)*, Revista de Direito Comercial, February 2020, pages 69-112, Available at: https://www.revistadedireitocomercial.com/responsabilidade-por-danos-e-inteligncia-artificial-ia, (Last accessed: 05.09.2021)

Goodman, Bryce; Faxman, Seth, 'European Union regulations on algorithmic decision-making and a "right to explanation', page 6, Available at: https://arxiv.org/pdf/1606.08813v3.pdf, (Last accessed: 05.09.2021)

Guimarães, Maria Raquel, *A tutela da pessoa e da sua personalidade: algumas questões relativas aos direitos à imagem, à reserva da vida privada e à reserva da pessoa íntima ou direito ao carácter*, *in A tutela geral e especial da personalidade humana — 2017* (Gabriela Cunha Rodrigues, Laurinda Gemas, Margarida Paz, orgs.), Lisboa, Centro de Estudos Judiciários, January 2018, pages 25-35

Guimarães, Maria Raquel, *A tutela da pessoa e da sua personalidade como fundamento e objecto da disciplina civilística – Questões actuais*, in Estudos Comemorativos dos 20 anos da FDUP, vol. II, Coimbra, Almedina, 2017, pages 291-311

Hamilton, Laura, "Six Novel Machine Learning Applications", Forbes, January 2014, Available at: https://www.forbes.com/sites/85broads/2014/01/06/six-novel-machine-learning-applications/?sh=1c16ad981060, (Last accessed: 05.09.2021)

Hao, Karen, "What is machine learning?", MIT Technology Review, November 2018, Available at: https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart/, (Last accessed: 05.09.2021)

High-Level Expert Group on Artificial Intelligence, "A definition of AI: Main capabilities and scientific disciplines", 2019

Hildebrandt, Mireille, "Location Data, Purpose Binding and Contextual Integrity: What's the Message?" contribution to Floridi, Luciano, Protection of Information and the Right to Privacy — A New Equilibrium?, Chapter 3, Law, Governance and Technology Series Volume 17 Springer, 2014. Available at: https://works.bepress.com/mireille_hildebrandt/54/, (Last accessed: 05.09.2021)

Iglezakis, Ioannis; Trokanas, Theodoros; Kiortsi, Panagiota, "The Right Not to Be Subject to Automated Individual Decision-Making/Profiling Concerning Big Health Data. Developing an Algorithmic Culture", March 2021, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3802771, (Last accessed: 06.09.2021)

Kaltheuner, Frederike; Bietti, Elletra, 2018. "Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR.", Journal of Information Rights, Policy and Practice, 2(2), DOI: http://doi.org/10.21039/irpandp.v2i2.45, (Last accessed: 05.09.2021)

Karanasiou, Argyro; Pinotsis, Dimitris, "A Study into the Layers of Automated Decision Making: Emergent Normative and Legal Aspects of Deep Learning." International Review of Law, Computers & Technology. 2016, Available at DOI: 10.1080/13600869.2017.1298499, (Last accessed: 05.09.2021)

Kritikos, Mihalis, "The impact of the General Data Protection Regulation (GDPR) on artificial intelligence", EPRS | European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 641.530, June 2020, Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf, (Last accessed: 05.09.2021)

Kroll, Joshua A.; Huey, Joana; Barocas, Solon; Felten, Edward W.; Reidenberg, Joel R.; Robinson, David G.; Yu, Harlan, "Accountable Algorithms", in University of Pennsylvania Law Review, vol. 165, 2017, pages 633-705, Available at: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9570&context=penn_law_review, (Last accessed: 05.09.2021)

Lohsse, Sebastian; Schulze, Reiner; Dirk, Staudenmayer, *Liability for artificial intelligence and the Internet of things* / ed. lit., Münster Colloquia on EU law and the Digital Economy IV, Hart Publishing, Nomos, 2019

Lufkin, Bryan, "10 grand challenges we'll face by 2050", BBC, July 2017, Available at: https://www.bbc.com/future/article/20170713-what-will-the-challenges-of-2050-be, (Last accessed: 05.09.2021)

MacCarthy, Mark; Propp, Kenneth, "Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation", Lawfare Institute, Brookings, Artificial Intelligence, April 2021 https://www.lawfareblog.com/machines-learn-brussels-writes-rules-eus-new-ai-regulation, (Last accessed: 05.09.2021)

Marr, Bernard, "8 Powerful Examples Of AI For Good", Forbes, February 2020 Available at: https://www.forbes.com/sites/bernardmarr/2020/02/10/8-powerful-examples-of-ai-for-good/?sh=1dcd13f0d18a, (Last accessed: 05.09.2021)

Matz, Sandra; Kosinski, Michael; Nave, Gideon; Stillwell, David, "Psychological targeting as an effective approach to digital mass persuasion", Proceedings of the National Academy of Sciences 114 (48): 201710966, November 2017, pages 1-6, Available at DOI:10.1073/pnas.1710966114, (Last accessed: 05.09.2021)

Medeiros, Rui; Miranda, Jorge, *Constituição Portuguesa Anotada*, Tomo I, Coimbra: Coimbra Editora, 2005

Mendoza, Isak; Bygrave, Lee Andrew, "The Right not to be Subject to Automated Decisions based on Profiling", University of Oslo Faculty of Law Legal Studies Research Paper Series No. 20/2017, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855, (Last accessed: 05.09.2021)

Mosier, Kathleen; Skitka, Linda; Heers, Susan; Burdick, Mark, *Automation Bias: Decision Making and Performance in High-Tech Cockpits,* The International journal of aviation psychology. 8.(1), February 1997, pages 47-63, Available at DOI: 10.1207/s15327108ijap0801_3, (Last accessed: 05.09.2021)

Mota Pinto, Paulo, *O Direito ao Livre Desenvolvimento da Personalidade*, in Boletim da Faculdade de Direito de Coimbra, Portugal-Brasil ano 2000, Coimbra Editora, 1999

Niemitz, Paul, "Constitutional democracy and technology in the age of artificial intelligence", The Royal Society, October 2018, Available at: https://royalsocietypublishing.org/doi/full/10.1098/rsta.2018.0089#FN2, (Last accessed: 05.09.2021)

Palmela, Vítor Fidalgo; Cordeiro, António Menezes, *Direito da proteção de dados : à luz do RGPD e da Lei n.º 58/2019* , Coimbra : Almedina, 2020

Papakonstantinou, Vagelis; De Hert, Paul, "EU law making in the Artificial Intelligent Age: Act-ification, GDPR mimesis, and regulatory brutality", July 2021, Available at: https://europeanlawblog.eu/2021/07/08/eu-lawmaking-in-the-artificial-intelligent-age-act-ification-gdpr-mimesis-and-regulatory-brutality/, (Last accessed: 05.09.2021)

Reis, Paulo Victor Alfeo, *Algoritmos e o direito*, São Paulo: Almedina, 2020

Roccas, Sonia; Sagiv, Lilach, "The Big Five Personality Factors and Personal Values", Sage Journals, Volume: 28 issue: 6, June 2002 Available at: https://journals.sagepub.com/doi/abs/10.1177/0146167202289008, (Last accessed: 05.09.2021)

Russell, Stiuart; Norvig, Peter, *Artificial Intelligence: A Modern Approach*, Prentice Hall, 3rd edition, 2009

Santos, Lourenço Noronha dos, *Inteligência Artificial e Direito*, § 12 Inteligência Artificial e Privacidade, Coordination Rocha, Manuel Lopes; Pereira, Rui Soares, Collaboration Ana Coimbra Trigo, Almedina, 2020

Sartor, Giovanni, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Scientific ForesightUnit(STOA)*,| Panel for the Future of Science and Technology, June 2020, Available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530, (Last accessed: 05.09.2021)

Schlatmann, Reinier, "COVID-19 and beyond: AI and health" , Politico, October 2020, Available here: https://www.politico.eu/sponsored-content/covid-19-and-beyond-ai-and-health/, (Last accessed: 05.09.2021)

The Danish Government, "National Strategy for Artificial Intelligence. Ministry of Finance and Ministry of Industry, Business and Financial Affairs.", 2019, Available at: https://eng.em.dk/media/13081/305755-gb-version_4k.pdf, (Last accessed: 05.09.2021)

UK Information Commissioner's Office: Data Protection Impact Assessments and AI, 23 October 2019, Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/, (Last accessed: 05.09.2021)

Ustaran, Eduardo, *European Data Protection: Law and Practice*, IAPP Publication, International Association of Privacy Professionals, 2018.

Veale, Michael; Edwards, Lilian, *Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling*, Computer Law & Security Review 34(2) 2018, pages 398-404, Available at: DOI: 10.1016/j.clsr.2017.12.002, (Last accessed: 05.09.2021)

Vinge, Vernor, "Technological Singularity, Whole Earth Review, Winter Issue, 1993, Available at: https://frc.ri.cmu.edu/~hpm/book98/com.ch1/vinge.singularity.html, (Last accessed: 05.09.2021)

Wachter, Sandra; Mittelstadt, Brent; Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", International Data Privacy Law, 2017, Vol. 7, No. 2., Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469, (Last accessed: 05.09.2021)

Wachter, Sandra; Mittelstdt, Brent, "A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI", April 2019, Available at: https://www.researchgate.net/publication/327872087_A_RIGHT_TO_REASONABLE_INFERENCES_RE-THINKING_DATA_PROTECTION_LAW_IN_THE_AGE_OF_BIG_DATA_AND_AI, (Last accessed: 10.09.2021)

Walker, Joshua, *IS "ETHICAL AI" A RED HERRING?*, 36 Santa Clara High Tech. L.J. 445, May 2020, Available at: https://digitalcommons.law.scu.edu/chtlj/vol36/iss4/1 (Last accessed: 07.09.2021)

Winston, Eric, "GDPR — How does it impact AI?", Information Age, Data Protection & Privacy, 19 June 2019

Woodruff, Allison, et al.,""A cold, technical decision-maker": Can AI provide explainability, negotiability, and humanity?" 1, 1, Association for Computing Machinery, December 2020, 23 pages, Available at: https://arxiv.org/pdf/2012.00874.pdf (Last accessed: 05.09.2021)

Zarsky, Tal Z., "Incompatible: The GDPR in the Age of Big Data", Seton Hall Law Review, Vol. 47:995, 2017

CASE LAW

Case AT.39740 — Google Search (Shopping), 27 June 2017, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1516198535804&uri=CELEX:52018XC0112(01).

Judgement of the European Court of Human Rights in the case Amann v Switzerland of 16.2.2000, Available at: http://hudoc.echr.coe.int/eng?i=001-58497.

Judgement of CJEU, C-615/13P, ClientEarth v PAN Europe.

Judgment of CJEU in Österreichischer Rundfunk and Others, C-465/00.

Judgment of CJEUC-138/01 and C-139/01, EU:C:2003:294.

Judgment of CJEU Worten, C-342/12, EU:C:2013:355.

INTERNET DAS COISAS (IOT) E O DIREITO DA PROTEÇÃO DE DADOS: UMA ANÁLISE DA APLICABILIDADE DO RGPD AOS DISPOSITIVOS INTELIGENTES

Ellis Bezerra de Mendonça Oliveira

Resumo: Nos primórdios, a internet foi concebida como uma rede entre computadores com o objectivo de criar um mundo virtual paralelo ao mundo real. A Internet das Coisas (*IoT*) surgiu nesse cenário para romper a fronteira entre esses dois mundos, por meio da conexão entre os diversos objetos do quotidiano a computadores e sensores, em um sistema ubíquo, que possibilita uma coleta massiva de dados do mundo real, o tratamento automatizado dessas informações e a tomada de decisões sem qualquer intervenção humana.

Os benefícios trazidos por essa nova realidade às mais diversas áreas vêm acompanhados de um impacto no conceito de privacidade e de uma série de questionamentos éticos acerca dos limites da penetrabilidade da inteligência artificial nas vidas humanas e dos riscos decorrentes da concentração de poder nas mãos dos controladores dos bancos de dados, sejam eles públicos ou privados.

O presente trabalho visa a analisar como as regras do Regulamento Geral de Proteção de Dados da União Europeia respondem às demandas originadas nesse novo cenário e em que medida são eficientes na consecução do propósito de proteger a privacidade dos titulares de dados sem impor pesados óbices ao desenvolvimento tecnológico.

Palavras-chave: Internet das Coisas, *IoT*, Privacidade, Proteção de Dados, Direitos da Personalidade, Regulamento Geral de Proteção de Dados, RGPD, Inteligência Artificial, Decisões automatizadas.

Abstract: In the beginning, the internet was created to function as a network between computers, emerging the virtual world in parallel to the real world. Then, the Internet of Things (*IoT*) was designed to break the boundary between these two worlds by interconnecting daily objects with computers and sensors, in a ubiquitous system, enabling a massive data collection, automated process of these information and decision-making without human interference.

This new reality brings benefits in many areas, but at the same time raises ethical questions about the limits of artificial intelligence penetration in human lives and about the risks of concentration of power in the hands of data controllers, whether public or private.

This paper aims to assess how the rules of EU General Data Protection Regulation respond to the issues arising in this new scenario and how efficient they are achieving the purpose of protecting the privacy of data subjects without imposing obstacles to the improvement of technology.

Keywords: Internet of Things, *IoT*, Privacy, Informational Privacy, Data Protection, Personality Rights, General Data Protection Regulation, GDPR, Artificial Intelligence, Automated Decision-making.

1. INTRODUÇÃO

O progresso tecnológico experimentado nas últimas décadas tem impactado substancialmente na vida das pessoas, fazendo surgir novas formas de comunicação, de produção, de transporte, de interação social. Desde o surgimento da internet, contudo, a importância da tecnologia na vida do homem comum tomou proporções inéditas e, a partir da Internet das Coisas, ganhou

concretude a realidade futurista das máquinas a "conviverem" com seres humanos em um mundo em que real e virtual são quase indissociáveis. Menos de três décadas desde a criação da World Wide Web (www), que popularizou o acesso à rede mundial de computadores, e hoje já não precisamos acessar a internet, pois vivemos a internet. Tamanha revolução social não viria sem nos impor consequências negativas ou diversos desafios éticos e jurídicos.

Neste trabalho, nos debruçamos sobre um pequeno recorte desse desafio, analisando o impacto da Internet das Coisas no que concerne ao direito à privacidade e, mais especificamente, à proteção dos dados pessoais.

Iniciamos, assim, na primeira parte, pelo estudo do elástico conceito de privacidade e sua evolução histórica, sempre a sofrer ajustes necessários a responder aos anseios sociais dominantes. Desse conceito, extraímos a noção de proteção dos dados pessoais, que embora originada nesse direito da personalidade à privacidade, nele não se esgota. Por fim, descrevemos o histórico da proteção jurídica garantida aos dados pessoais, definindo o contexto jurídico no qual surgiu o atual Regulamento Geral de Proteção dos Dados (RGPD) vigente na União Europeia, mas com inquestionável impacto em todo o mundo digital.

Na segunda parte, cuidamos de conceituar brevemente a Internet da Coisas (IoT) e os elementos tecnológicos que a fizeram possível e/ou a potencializaram, como a inteligência artificial, o machine learning e o Big data. A partir daí, analisamos a aplicabilidade do RGPD aos dispositivos IoT, apresentando o enquadramento jurídico dessa realidade.

Já na terceira parte, voltamos os olhos ao RGPD e apresentamos uma leitura dos seus objetivos, princípios e conceitos sob a óptica tecnológica da Internet das Coisas. Destacamos, outrossim, as peculiaridades dessa realidade tecnológica e como suas características impactam na interpretação e aplicação do Regulamento.

Por fim, apresentamos alguns dos principais desafios a serem enfrentados para aplicação prática das regras do RGPD aos dispositivos inteligentes e às tecnologias a ele associadas, descrevendo os pontos de aparente incompatibilidade entre os avanços tecnológicos e as regras e princípios do Regulamento.

2. A PROTEÇÃO JURÍDICA DOS DADOS PESSOAIS: O CONTEXTO HISTÓRICO DO RGPD

2.1. A EVOLUÇÃO DO CONCEITO DE PRIVACIDADE E SUA PROTEÇÃO COMO DIREITO DA PERSONALIDADE

O conceito de privacidade, significando algo de acesso restrito em contraponto ao que é de domínio público, remonta à antiguidade clássica. Embora na Grécia antiga Aristóteles já falasse na existência da *esfera pri-*

vada ("oikos") e da *esfera pública* ("polis"), foi dos romanos que herdamos o vocábulo *privatus*, raiz etimológica de *privacidade*[1]. Para os antigos, o âmbito privado, para além da família, abarcava igualmente questões económicas, diferentemente do âmbito público, relativo às relações comunitárias e à vida do cidadão na *polis*.

Note-se que desde então o conceito de "privado" nasce de um critério negativo em relação ao que é público. Representa, assim, um conjunto de coisas agregadas por terem em comum o fato de não serem identificadas como algo de interesse ou domínio público. Essa dicotomia público-privada foi, com o tempo, sendo associada a outra: vida pessoal (homem singular ou família) *versus* vida social ou comunitária[2]. Por isso, ao poucos, o termo *privacidade* passou a abarcar tudo aquilo que se afastava da vida comunitária e estava relacionado com a individualidade do homem ou com o seu núcleo social mais íntimo: a família.

Segundo Bioni[3], a habitação representaria o ambiente privado (o homem em seu castelo). A casa, assim, seria um ambiente reservado à reflexão e ao pensamento crítico, antecessores necessários às discussões que teriam lugar no espaço público. Esse refúgio, segundo o autor, protege o indivíduo contra a instalação de visões totalitárias, sendo o direito à privacidade basilar à democracia e condição essencial ao livre desenvolvimento da personalidade[4].

Tal distinção ostentava uma consequência decisória, por caber ao *homem* e não à *polis* decidir sobre sua esfera privada e determinar os rumos de suas vidas naquilo que não dissesse respeito à vida comunitária. Com o tempo, a *privacidade* foi estreitando os laços de conteúdo com o conceito de liberdade, já que, na esfera privada, cabia ao indivíduo escolher livremente seu modo de agir. Esse pensamento encontra seu apogeu no Iluminismo, notadamente com ascensão do pensamento liberal, como ensina Correia[5].

Os limites do conceito de *privacidade*, contudo, ganham contornos diferentes a depender do momento histórico e cultural considerado. Ora, sendo privado tudo o que não é público, é de se concluir que o conteúdo da esfera privada variará ao longo da história e estará relacionado aos diversos arranjos políticos adotados e ao grau de transferência de poder da esfera individual para o Estado, em benefício da coletividade e do interesse público. Por esse motivo, o vocábulo *privacidade* tem como característica intrínseca certa elasticidade e imprecisão, não sendo possível extrair dele um significado estanque sem ter em consideração o momento histórico e a forma

---

1 Victor Correia, *Sobre a Privacidade*, Editora Sinapsis, 2016, p. 63.

2 Paulo Mota Pinto fala que a privacidade se baseia em uma *tensão entre o social e o individual*. Paulo Mota Pinto, *Direitos de Personalidade e Direitos Fundamentais: estudos*, Coimbra, Gestlegal, 2018, p. 509.

3 Bruno Ricardo Bioni, *Proteção de Dados Pessoais: a função e os limites do consentimento,* Rio de Janeiro, Forense, 2019.

4 Bruno Ricardo Bioni*, Op. Cit*., p. 93.

5 Victor Correia, *Op. Cit.*, p. 64.

de abordagem do tema (se sob a perspectiva jurídica, filosófica, política)[6]. Dessa elasticidade decorre a impossibilidade de definir os contornos de um bem jurídico: por um lado, reflete sua amplitude, por outro pode resultar em uma nebulosidade, como as ideias de "felicidade" e "segurança"[7], que impede ou dificulta sobremaneira a proteção legal.

Como tentativa de segmentar os vários extratos da privacidade, para fins de estabelecer o grau de sigilo e a proteção merecida, foi elaborada a teoria das esferas, creditada a Heinrich Hubmann, na obra "Das Persomlichkeitrecht", de 1953. O autor propõe em termos de profundidade do grau de privacidade a ilustração representada por três círculos concêntricos, caracterizando, do mais restrito para o mais abrangente, a "esfera individual", a "esfera privada" e a "esfera secreta"[8].

Em linhas gerais, o que é "individual" corresponde ao homem integrado ao meio social, como seu "carácter", sua "personalidade", dando ensejo ao "direito a ser socialmente respeitado na sua individualidade" e a uma resistência contra a "massificação" do indivíduo. Já as esferas "privada" e "secreta" representam a necessidade de proteção de certos aspetos da vida contra a invasão pública e a "curiosidade". Segue Pinheiro a defender ser na "área secreta" que se desenvolvem os pensamentos, opiniões, descrição de sensações e tudo aquilo que as pessoas desejam manter em reserva e possuem interesse no seu segredo[9].

Já Paulo Mota Pinto esclarece que a definição de privacidade pressupõe, em um primeiro momento, a sua distinção em relação a outros interesses com os quais por vezes é confundida. Por isso, o autor cuida de excluir do conceito de privacidade noções relativas à liberdade de condução da própria vida, assim como a reputação, o bom nome e a livre fruição de atributos pessoais[10]. Por outro lado, numa perspectiva positiva, Mota Pinto enumera três interesses abrangidos pelo conceito de privacidade: o controlo sobre as informações pessoais, a subtracção da atenção dos outros (anonimato) e a solitude[11]. Para além disso, a privacidade é a estrutura que garante o desenvolvimento da individualidade e das relações humanas de confiança. Por isso, é comumente associada com um aspecto da dignidade humana[12].

Em terras norte-americanas, é considerado marco da proteção jurídica da privacidade o artigo *The Right of Privacy*, de autoria de Warren e Brandeis e

---

6 Paulo Mota Pinto, *Op. Cit.,* p. 503.

7 Paulo Mota Pinto, *Op. Cit.,* p. 504.

8 Alexandre Sousa Pinheiro, Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional, Lisboa, AAFDL, 2015.

9 Alexandre Sousa Pinheiro, *Op. Cit.,* p. 448.

10 Paulo Mota Pinto, *Op. Cit,* p. 505..

11 Paulo Mota Pinto, *Op. Cit.*, p. 507.

12 Paulo Mota Pinto, *Op. Cit.*, p. 508.

publicado em 1890 na *Havard Law Review*[13]. Na época, nos Estados Unidos da América, experimentava-se o avanço da imprensa, popularizada, massificada e incrementada pela possibilidade de ilustração com fotografias. Conforme descreve Pinheiro[14], a partir de 1860, os jornais passaram a publicar entrevistas que se revelavam no mais das vezes uma devassa à intimidade da pessoa, embora de forma consentida, pois o entrevistado anuía com as perguntas. Outro elemento citado pelo autor consiste na invenção de George Eastman, responsável pelo lançamento das máquinas de fotografar *hand-handle Kodak*. Sob o *slogan* "You press the button, we do the rest", os dispositivos se popularizaram e o ato de fotografar passou a significar mais um novo meio de invasão da privacidade, notadamente mediante especulação e exposição da vida de pessoas socialmente relevantes[15].

É nesse contexto que Warren e Brandeis traçam uma interpretação de precedentes da *common law* com o objetivo de apresentar como ilícito civil (*tort)* a conduta de entidade privadas (imprensa) ao expor fatos da vida privada de alguém ou fotografias não autorizadas. Assim, a *privacy* americana, como um direito, foi construída pelos autores a partir do *right to be let alone*, extraindo dele uma interpretação condizente com o novo contexto social e estendendo seu conteúdo de modo a permitir a proteção dos indivíduos frente às invasões da imprensa. A partir daí, o *right to privacy* passou a ser reconhecido pela jurisprudência e consagrado nas leis, com contornos conceituais amplos, inclusive fundamentando decisão da Suprema Corte, em 1965, sobre a possibilidade de proibir o uso de contraceptivos (caso *Griswold* contra *Connecticut*)[16].

A ampla abrangência da *privacy* americana permitiu, portanto, que o direito à privacidade servisse de fundamento tanto para a restringir as formas de tornar pública uma informação pessoal (*informational privacy*), quanto para garantir a liberdade do indivíduo de conduzir sua própria vida, por meio de atos autodeterminados de conteúdo social, cultural, ético ou moral (*decisional privacy*)[17]. Por isso, o *right to privacy* nos Estados Unidos inspirou ao mesmo tempo o *Privacy Act* (lei federal com o fim de proteger o controlo da informação contra atos de entidades públicas) e decisões judiciais sobre os mais variados assuntos, como a inconstitucionalidade de leis que proíbem

---

13 Samuel D. Warren e Louis D. Brandeis, "The Right To Privacy*" in Harvard Law Review*, nº 5, Vol. IV, 1890, pp. 193-220.

14 Alexandre Sousa Pinheiro, *Op. Cit.,* pp. 276-278.

15 Paulo Mota Pinto descreve as razões pelas quais os problemas relacionados à privacidade foram objeto de preocupação na sociedade americana: a agressividade da imprensa, o abismo tecnológico entre a realidade americana e a dos demais países e, ainda, os valores fundamentais daquela sociedade, mormente a especial relevância da defesa do indivíduo. Paulo Mota Pinto, *Op. Cit.*, p. 512.

16 Paulo Mota Pinto, *Op. Cit*., p. 513.

17 Alexandre Sousa Pinheiro, *Op. Cit.*, pp. 365/366.

o aborto, a permissão do "direito a morrer" e a permissão do uso de cabelos compridos por certos profissionais[18].

Já na Europa, o direito à privacidade se desenvolveu a partir do reconhecimento dos direitos da personalidade, cuja proteção jurídica autônoma remonta ao século XIX[19]. Partiu-se, portanto, da premissa de conceber a pessoa humana como titular de uma série de direitos protetores dos bens da personalidade. A origem dessa proteção, todavia, é, como dissemos, atribuída ao Direito Romano, que já previa salvaguardas à honra, à reputação e à dignidade, bens que permaneceram sob proteção em boa parte dos países europeus durante os séculos XVIII e XIX[20]. Tais bens, inerentes a toda pessoa e essenciais ao livre desenvolvimento da personalidade, comporiam uma espécie de patrimônio imaterial e dentre eles estariam, por exemplo, o direito à imagem e o direito à vida privada[21].

Com marco jurisprudencial europeu, Pinheiro[22] cita as decisões francesas do "Tribunal Civil de la Seine", ambas em proteção ao *droit à la vie privée*, uma que "*proibiu a exibição pública de um quadro que representava a Madre Superior das Irmãs de Providência*", em 1855, e a outra que tratou da "*publicação de imagens (desenhos e pinturas) ilustrando a atriz Rachel Félix no seu leito de morte"*, em 1858.

Mas foi principalmente após a Segunda Guerra Mundial, com o fenômeno da "despatrimonialização do Direito Civil[23], que as demandas impostas pelas circunstâncias fáticas[24] impulsionaram a proteção legal aos direitos da personalidade, sobretudo na Alemanha, onde, em 1954, a jurisprudência construiu o "direito geral de personalidade", a partir da interpretação conjunta do §823, n.º 1.º do BGB e da dignidade da pessoa humana (art. 2.º, n.º 1.º, da Lei Fundamental da República da Alemanha de 1949) (caso *Lesebrief*)[25], para concluir pela impossibilidade de publicação de notas pessoais sem o consentimento de autor vivo.

A proteção da personalidade por meio de um direito geral a englobar todos os aspectos da personalidade constituiu um sistema adotado não só pela Alemanha, mas também por outros países europeus como Itália e Áustria. A vantagem apontada para o sistema reside na sua abrangência, que permite o

---

18 Paulo Mota Pinto*, Op. Cit*., p. 514.

19 Paulo Mota Pinto*, Op. Cit*., p. 478.

20 Eva Ondreasova, "Personality Rights in Different European Legal Systems: Privacy, Dignity, Honour and Reputation.", *in The Legal Protection of ersonality Rights: Chinese and European perspectives*. Ken Oliphant, Zhang Pinghua, e Chen Lei. Leiden, Brill, 2018. pp. 24-70.

21 Alexandre Sousa Pinheiro, *Op. Cit.*, pp. 432 e seguintes.

22 Alexandre Sousa Pinheiro, *Op. Cit.*, p. 436.

23 Bruno Ricardo Bioni, *Op. Cit.*, p.55.

24 Nesse tocante, não apenas o cenário pós-guerra e derrota nazista, mas o desenvolvimento tecnológico, com a invenção do computador e a democratização da fotografia e da imprensa, tudo contribuindo para a transformação da pensonalidade como um bem economicamento valioso, conforme descrição de PINHEIRO, Alexandre Sousa. *Op. Cit.*, p. 435.

25 Alexandre Sousa Pinheiro, *Op. Cit*., p. 438.

desenvolvimento do direito de acordo com as mudanças tecnológicas e sociais. Todavia, há críticas ao modelo, notadamente ante a dificuldade de se estabelecer os contornos do instituto e à insegurança jurídica daí decorrente[26].

Por outro lado, países como a França optaram pela proteção aos diversos direitos da personalidade separadamente, inclusive o direito à privacidade, ambos expressamente incluídos no Código Civil francês em 17 de Julho de 1970[27]. O modelo, também adotado por países com Suécia e Reino Unido, embora permita uma melhor diferenciação entre as diferentes facetas dos direitos da personalidade, na prática pode resultar na existência de lacunas e contradição entre valores[28].

Em Portugal, o artigo 70.º, n. 1.º, do Código Civil de 1966 representa salvaguarda aos direitos da personalidade, através de uma cláusula geral, a fim de proteger os indivíduos *contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral*. O dispositivo serve como espécie de "direito-quadro" a abranger bens da personalidade não tipificados, do modo "aberto" sincrónica e diacronicamente[29]. Além disso, o Código Civil português também prevê a proteção de direitos da personalidade específicos, como o direito sobre o conteúdo de cartas-missivas e outros escritos (artigos 75.º a 78.º), o direito à imagem (artigo 79.º) e o direito à reserva sobre a intimidade da vida privada (artigo 80.º)[30].

Alerta Orlando de Carvalho, contudo, que o direito geral da personalidade não deve ser confundido com uma mera ferramenta para superação das lacunas deixadas pela previsão dos direitos de personalidades especiais, tampouco como a condensação desses direitos em um único dispositivo. Deve servir, assim, o direito geral da personalidade como fundamento axiológico para as demais disposições legais, como referencial interpretativo, portanto[31].

Em relação ao direito à privacidade propriamente dito, importa destacar sua proteção específica prevista na Convenção Europeia dos Direitos do Homem (artigo 8.º), de 1950, bem como nos Códigos Civis de França e de Portugal[32]. Em Portugal, como também em Espanha, há ainda proteção constitucional ao direito à privacidade, nomeadamente no artigo 26.º[33].

Em geral, a proteção à privacidade abrange a defesa da esfera privada e da intimidade, principalmente em assuntos relacionados à saúde, sexualidade e vida familiar. Em alguns casos também incluída nesse rol a proteção ao anoni-

---

26 Eva Ondreasova, *Op. Cit*., p. 49.

27 Eva Ondreasova, *Op. Cit*., p. 34.

28 Eva Ondreasova, *Op. Cit*., p. 50.

29 Paulo Mota Pinto, *Op. Cit*., pp. 493/494

30 Paulo Mota Pinto, *Op. Cit*., p. 498

31 Orlando de Carvalho, *Teoria Geral do Direito Civil,* 3ª ed, Coimbra, Coimbra Editora, 2012, p. 263.

32 Eva Ondreasova, *Op. Cit*., p. 57.

33 Paulo Mota Pinto, *Op. Cit*., p. 521.

mato[34]. Em Portugal, especificamente, o Código Civil preferiu o uso da expressão "intimidade da vida privada", representando, por si, um recorte ao amplo direito à privacidade[35]. Para Mota Pinto, a dicção legal resulta na exclusão não só dos eventos próprios da "vida pública" de alguém, mas também de aspectos da vida privada não íntimos, por exemplo, os segredos dos negócios[36].

Para estabelecer a fronteira entre a vida pública e a privada do indivíduo, deve-se recorrer a critérios que se tornarão mais ou menos eficientes a depender do contexto em que são aplicados[37]. Por exemplo, o critério espacial pode-se mostrar eficiente para garantir a proteção de informações próprias do ambiente doméstico, sendo certo, contudo, que alguns eventos privados poderão ter lugar em ambientes públicos. Por outro lado, a tecnologia permitiu um maior acesso a esses ambientes íntimos objeto de reserva, seja pela variabilidade de novas ferramentas a permitirem a intrusão de terceiros, seja pela possibilidade de o próprio indivíduo divulgar publicamente informações íntimas.

Assim, vê-se que apesar de a proteção da privacidade não estar necessariamente ligada à tecnologia, o desenvolvimento tecnológico tornou ainda mais premente a necessidade de proteção legal da privacidade, pois hoje existem meios consideravelmente mais eficazes de violação da intimidade, sobretudo quando consideramos a penetrabilidade de sensores, microfones e câmeras, objetos atualmente omnipresentes[38]. Logo, hoje o contexto tecnológico é preponderante para definir os contornos do conceito de privacidade, de modo que, sem considerá-lo, a proteção legal não conseguirá responder às demandas atuais nem se adaptar às novas ameaças.

2.2. O DIREITO À PROTEÇÃO DOS DADOS PESSOAIS

Apesar de os contornos conceituais e doutrinários da proteção de dados já estarem fixados desde antes – com a evolução do conceito de privacidade e o reconhecimento da necessidade de se proteger a individualidade e controlar o acesso e a divulgação de informações pessoais – foram os avanços tecnológicos da segunda metade do século passado e a capacidade de tratamento de dados em escala inédita, com possibilidade de cruzamento de

---

34 Eva Ondreasova, *Op. Cit*., pp. 61/62.

35 Maria Raquel Guimarães e Maria Regina Redinha, "Through the Keyhole: Privacy in COVID-19 Times — A Portuguese Approach." *in Intersentia Online*, 2020, disponível em https://www.intersentiaonline.com/publication/coronavirus-and-the-law-in-europe/2 (Consulta em 01.08.2021)

36 Paulo Mota Pinto, *Op. Cit*., p. 532.

37 O contexto nesse caso deve ser avaliado não só considerando cada indivúduo caso a caso, mas também em função das valorações de cada formação social, conforme ensina Paulo Mota Pinto, *Op. Cit*.

38 Paulo Mota Pinto, *Op. Cit.,* p. 511.

informações de origens diversas, que elevaram a importância do tema[39] a ponto de ser considerado urgente algum tipo de regulamentação específica, desmembrada da genérica proteção da privacidade.

Para Mafalda Barbosa, a popularização do uso da informática resultou na democratização do risco antes existente em relação aos poderes públicos, em razão da concentração de informações em poder do Estado. Hoje, a utilização de modernos sistemas de informação e a possibilidade de compartilhamento de dados entre eles permite a qualquer particular a articulação de diversas informações acerca de um mesmo indivíduo, o que aprofundou a necessidade de regulação específica do acesso, tratamento e transmissão dos dados pessoais[40].

Sobre o assunto, destaca-se a categorização das normas de proteção de dados em *quatro gerações,* a depender do seu escopo: proteção do indivíduo contra o processamento massivo de dados pelos Estado (*primeira geração)*, ampliação da proteção também em relação a bancos de dados não estatais (*segunda geração*), deslocamento do papel de protagonismo do Estado para o indivíduo através do consentimento (*terceira geração*) e a articulação entre o protagonismo do consentimento do titular com a aplicação das leis por autoridades independentes[41].

Nos Estados Unidos, o termo *privacy* já foi concebido, com vimos, com amplo escopo. Extraído a partir do *right to be let alone*, a proteção da privacidade serviu de fundamento para decisões jurisprudenciais tanto relacionadas à *informacional privacy*, quanto à *decisional privacy*, de modo que o direito da proteção dos dados se confunde com a própria tutela da privacidade.

Na Europa, por outro lado, conforme descreve Bioni, o conceito de privacidade teria se alargado de modo a abarcar, para além de sua faceta estática, uma feição dinâmica correspondente à proteção dos dados pessoais e sua prerrogativa de controlo das informações pelo titular (autodeterminação informativa)[42]. Porém, o autor defende que isso não significa dizer que o direito à proteção de dados pessoais deve ser reduzido a uma mera evolução do direito à privacidade, pois ele possui autonomia própria. Prova disso é que o direito à proteção de dados rompe com a dicotomia entre o público e

---

39 Herminia Campuzano Tomé. Vida Privada y Datos Personales: Su Protección Jurídica Frente a La Sociedad de la Información, Madrid, Tecnos, 2000, p. 71.

40 Mafalda Miranda Barbosa, "Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil.", *in Estudos de Direito do consumidor*, n.º 12, Coimbra, Centro de Direito do Consumo/ FDUC, 2017, pp. 75-131.

41 Bruno Ricardo Bioni, *Op. Cit.,* pp. 115-117.

42 Bruno Ricardo Bioni, *Op. Cit.,* p. 93 Para o autor, o conceito tradicional de privacidade possui característica estática, pois define *a priori* quais fatos estão ou não incluídos na esfera privada do indivíduo. Por outro lado, a proteção de dados representaria uma perspectiva dinâmica de privacidade ao passo que entrega ao indivíduo a liberdade positiva de controlar suas próprias informações.

o privado, passando o bem jurídico a estar associado ao conceito de dado pessoal[43]. Para o autor, o direito à proteção de dados pode ser inserido no rol dos direitos à personalidade, pois os dados pessoais constituem uma projeção da pessoa humana[44].

Já Barreto Menezes Cordeiro, sem negar importância dos direitos da personalidade como fundamento para o direito da proteção de dados, ensina que esse novo direito vai além de simplesmente proteger os interesses dos titulares, estabelecendo os critérios essenciais para garantir a livre circulação dos dados pessoais[45].

Em termos de regulamentação própria, o marco inicial do Direito da proteção de dados é considerado a criação, pelo Congresso dos Estados Unidos da América, do *Special Subcommittee on Ivasion of Privacy*, em 1965[46]. O *Special Subcommittee* realizou uma série de audiências tendo, primeiramente, o foco de investigar supostas prática violadoras da *privacy* por agências federais. Mas a partir de 1968, os trabalhos voltaram-se também a entidades privadas, notadamente agências de crédito, responsáveis à época pela elaboração de verdadeiros dossiês que descreviam o perfil de cada cliente.

Sobre o assunto, ensina Barreto Menezes Cordeiro ter a preocupação, na época, emergido do fato de esses relatórios individuais conterem, muitas vezes, informações incorretas, irrelevantes e viciadas ou, ainda, invadirem desarrazoadamente a esfera pessoal e secreta. Além disso, os dossiês elaborados pelas agências de crédito impactavam de modo substancial a vida dos titulares dos dados por determinarem o seu acesso ao crédito, por exemplo, e até mesmo influenciarem na contratação de um seguro ou na seleção para ocupar um posto de trabalho. O desenvolvimento da Sociedade de Consumo, com a procura maciça por crédito, levou a uma generalização dessa prática e tornou ainda mais urgente a necessidade de regulamentação específica[47]. Os resultados legislativos do *Special Subcommittee* vieram mais tarde com a aprovação do *Fair Credit Reporting Act* (1970)[48] e o *Privacy Act* (1974)[49].

---

43 Bruno Ricardo Bioni, *Op. Cit.,* pp. 97/98.

44 Bruno Ricardo Bioni, *Op. Cit.,* pp. 63-65.

45 António Barreto Menezes Cordeiro, *Op. Cit.,* p. 33.

46 António Barreto Menezes Cordeiro, *Op. Cit.,* p. 53

47 Para ilustrar esse cenário, o Professor faz referência às palavras de Hillel Black, escritas em 1961: "If your name is not in the records of at least one credit bureau, it doesn´t mean you don´t rate. What means is that you are either twenty-one or dead". António Barreto Menezes Cordeiro, Op. Cit.

48 Tinha por escopo proteger o particular contra a coleta de informações incorretas, estabelecer poderes de fiscalização ao *Federal Trade Commission (FTC)* e impor responsabilidades a quem desenvolve esta atividade. Em resumo, "*para assegurar que agências exerçam suas sérias responsabilidades com justiça, imparcialidade, e respeito pelo direito do consumidor à sua privacidade*", conform dicção do §602 do *Fair Credit Reporting Act* em tradução livre.

49 Regula o tratamento de dados no âmbito dos órgãos governamentais, tendo o intuito de estabelecer salvaguardas ao cidadão contra a invasão de privacidade por agências federais.

Para Barreto Menezes Cordeiro, o *Privacy Act* estabelece um conjunto de princípios que hoje representam o núcleo do Direito da proteção de dados[50]. De fato, do documento é possível extrair o protagonismo do titular de dados em relação à atividade de tratamento, sobretudo por estabelecer seu direito de acesso a quais dados seus estão sendo tratados e com quais finalidades, bem como deveres das agências federais como o de restringir a atividade de tratamento de dados pessoais a propósitos necessários e legais, respeitada a finalidade, garantida a atualidade da informação e evitado o seu mau uso (em tradução livre do texto normativo "*misuse"*).

No que toca ao Direito estado-unidense é o que importa aos propósitos do presente trabalho destacar, sendo digno de menção entretanto que diversos outros diplomas foram aprovados desde então com impacto na temática de proteção dos dados com aplicações limitadas a certo estado daquela Federação ou a certos setores tais como *Family Educational Rights and Privacy Act* (1978), *Right to Finantioal Privacy* (1978)*, Privacy Protection Act* (1980), *The Electronic Communications Privacy Act* (1986).

Já na Europa, os primeiros traços partem da jurisprudência alemã, onde cunhou-se pela primeira vez o termo *Datenschutz* (proteção dos dados em tradução livre para o português). Note-se que dadas as diferenças de evolução do conceito nos diferentes ordenamentos jurídicos, a proteção de dados europeia não corresponde exatamente à *privacy* americana, embora sejam comumente tratadas como sinônimo. Conforme ensinamentos de Pinheiro, a *Datenschutz* pode ser correlacionada, em linha gerais, com a *informational privacy*, mas essa correlação não exacta, até pelo fato de a proteção de dados europeia abranger certos interesses não resguardados pelo direito estado-unidense, razão pela qual a Europa não reconhece como *adequada* a proteção garantida pelos americanos[51].

A decisão partiu da análise da constitucionalidade da Lei dos Censos de 1983. Segundo a lei alemã, todos os cidadãos consentiriam na coleta de dados pessoais para fins estatísticos, sendo previsto também, de forma genérica e sem especificar a finalidade, o cruzamento desses dados com outros contidos em bancos de dados públicos na execução de atividades administrativas. A partir do art. 2.º, n.º 1, (livre desenvolvimento da personalidade) e o art. 1.º, n.º 1 (dignidade da pessoa humana), ambos da Constituição Alemã, e decidiu-se pela existência do direito do indivíduo de ser protegido contra "*a recolha, armazenamento, uso e transmissão ilimitados de dados pessoais"*[52].

Para Pinheiro, a fundamentação do julgado alemão, que ainda não tratava expressamente de autodeterminação informativa, é paradigmática justamente por dissociar o direito à privacidade e o direito à proteção de dados e não resumir esse último a uma mera evolução do primeiro, justificando a impor-

50 António Barreto Menezes Cordeiro, *Op. Cit.*, p. 59

51 Alexandre Sousa Pinheiro, *Op. Cit*., p. 428/429.

52 Alexandre Sousa Pinheiro, *Op. Cit.,* p. 479.

tância em não confundir esse conceito com o da *privacy* no contexto americano[53]. Ademais, a importância da Decisão dos Censos vai além da construção do princípio da especificação dos propósitos, pois também rompe com a ideia do protagonismo do consentimento com meio de legitimação do tratamento de dados, mormente a posição de assimetria do cidadão frente ao Estado[54].

Essa independência do direito à proteção de dados em relação ao direito à privacidade tem uma relevância indiscutível para o desenvolvimento do tema até os patamares regulatórios atuais. Primeiro, por servir de base à conclusão de que o simples consentimento não pode ter o condão de justificar todo e qualquer tratamento, sob pena de transformar a pessoa em "*objeto a ser ilimitadamente explorado*"[55]. Segundo, por ampliar o alcance dessa proteção[56].

2.3. A PROTEÇÃO JURÍDICA DOS DADOS PESSOAIS

Os mais variados meios de produção adotados pelas sociedades ao longo da história sempre impactaram no valor de determinados bens e, por consequência, no grau de proteção jurídica direcionadas aos bens considerados pilares da estrutura econômico-social. Foi assim com as terras, no período eminentemente agrícola; com os parques industriais (seja de fabricação de bens, seja de produção de energia), no período da primeira revolução industrial; com os estabelecimentos comerciais, na sociedade pós-industrial.

Por sua vez, o aprofundamento da complexidade da teia social, atrelado ao desenvolvimento de novas tecnologias – de modo veloz e irreversível – trouxe-nos até o momento presente: o da era da informação, na qual tem mais poder quem detém "os dados". Nesse contexto, houve um aumento exponencial da atividade de coleta de dados e, para o mercado, os bancos de dados passaram a ser considerados ativos cada vez mais valiosos[57]. Assim como nos períodos históricos anteriores em relação aos respectivos "bens-pilares", o arcabouço normativo referente aos dados assume especial significado, pois, para além de regular o acesso a um bem jurídico economi-

---

53 Alexandre Sousa Pinheiro, *Op. Cit.,* p. 487.

54 Bruno Ricardo Bioni, *Op. Cit.,* pp. 104-106.

55 Bruno Ricardo Bioni, *Op. Cit.,* p. 106.

56 A título de comparação, Bioni remete a uma decisão anterior do mesmo tribunal alemão em relação à Lei do Microcenso de 1957 a qual centrou-se na fundamentação de que, em aplicação ao direito à privacidade, a coleta de dados para ser considerada ilegítima deveria violar a esfera íntima do cidadão. Bruno Ricardo Bioni, *Op. Cit*., p. 106.

57 Seja por exploração direta por meio da publicidade direcionada, seja por constituir importante fonte de informação sobre o consumidor, conforme conclui Marília de Mello e Silva Corôa, *O Mercado De Dados: Estrutura, Funcionamento e o Reflexo do RGPD no Novo Mercado à Base De Dados Pessoais.* Dissertação (Mestrado em Ciências Jurídico-civilísticas), Faculdade de Direito da Universidade do Porto, Porto, 2020, p. 51.

camente relevante, passa a representar a proteção mesma do indivíduo, da sua vida e da sua liberdade[58].

No que toca especificamente aos dados pessoais, a sua proteção no direito português remonta ao legislador constitucional de 1976, que já lhe garantiu proteção (art. 35.º), ainda que remetendo a definição de "dados pessoais" à legislação ordinária[59]. A previsão representa a autonomia do direito da proteção de dados em relação à proteção da intimidade da vida privada, consagrada no art. 26.º da Constituição Portuguesa. Ainda, do texto legal extrai-se que proteção dos dados pessoais vai além daquelas informações relativas à vida privada, em relação às quais há especiais exigências (art. 35.º/3)[60]. Ainda que de forma embrionária, se comparada com a sistematização positivada mais tarde pelo RGPD, o art. 35.º da Constituição foi pioneiro ao estabelecer os direitos dos titulares de dados como o *direito de acesso*, o *direito ao não tratamento de dados sensíveis* e o *direito ao sigilo dos dados*[61].

A definição de "dados pessoais" pela legislação infraconstitucional viria apenas em 1991 com a Lei da Protecção de Dados Pessoais face à Informática (Lei n.º 10/91, de 27 de Abril), cujas disposições se aplicavam "À constituição e manutenção de ficheiros automatizados, de bases de dados e de bancos de dados pessoais" e "*Aos suportes informáticos relativos a pessoas colectivas e entidades equiparadas, sempre que contiverem dados pessoais*"[62]. Essa primeira legislação teve vigência até 1998, quando foi revogada pela Lei n.º 67/98, de 26 de Outubro, responsável pela transposição da Diretiva 95/46/CE[63].

Já no direito europeu, o marco legislativo relativo a proteção dos dados pessoais é associado à Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares, de 28 de janeiro de 1981, primeiro ins-

---

58 A importância que os dados representam para Era Digital é retratada na expressão "os dados são o novo petróleo", conforme ensina António Barreto Menezes Cordeiro, *Op. Cit.,* p. 29.

59 A redação original do Artigo 35.º contava com apenas três números, um referente ao direito do cidadão de "de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização" (n.º 1) e os outros dois referentes às proibições de tratamento de dados relativos à convicções políticas, fé religiosa ou vida privada (n.º 2) e de atriubuição de número nacional único aos cidadãos (n.º 3). Apenas após as revisões constitucionais de 1982, 1989 e 1997 o texto constitucional alcança a atual redação, conforme detalha Catarina Sarmento e Castro, "40 anos de "Utilização da Informática" — O artigo 35.º da Constituição da República Portuguesa", in Revista e-Pública, n.º 3, Vol. 3, 2016, disponível em https://www.e-publica.pt/volumes/v3n3a04.html (Consulta em 01.08.2021)

60 Catarina Sarmento e Castro, *Op. Cit.,* p. 50.

61 Carlos André Ferreira Dias. *A Privacidade na era da Internet das Coisas: direitos de personalidades e proteção de dados.* Dissertação (Mestrado em Ciências Jurídico-civilísticas) Faculdade de Direito da Universidade do Porto, Porto, 2019, p. 22.

62 Art. 3.º, n.º 1, da Lei n.º 10/91.

63 Mafalda Miranda Barbosa, *Op. Cit.*, pp. 75-131.

trumento internacional juridicamente vinculativo[64] adotado sobre a matéria, "*(...) resultado do movimento promovido pela OCDE para facilitar a harmonização das legislações de proteção dados pessoais."*[65]. A importância do tema consagrou-se, posteriormente, com sua inclusão na Carta dos Direitos Fundamentais da União Europeia (artigo 8.º)[66] e no Tratado sobre o Funcionamento da União Europeia (artigo 16.º)[67].

De forma sistematizada, outrossim, a matéria foi tratada pela primeira vez pela Diretiva 95/46/CE, transposta em Portugal pela Lei n.º 67/98, em vigor até ser revogada pelo Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, ou Regulamento Geral de Proteção de Dados (RGPD), que representa a concretização da relevância reconhecida à proteção dos dados, não só em uma perspectiva econômica (reforço da confiança para o consumo digital e da competitividade das empresas com postura responsável em relação às políticas de privacidade), mas também de proteção dos direitos de personalidade, sobretudo à privacidade.

Sobre o assunto, Barreto Menezes Cordeiro ressalta o impacto do Direito da proteção de dados na vida quotidiana provocado pelos avanços tecnológicos significativo das últimas décadas e a posição de fragilidade do indivíduo frente aos mais variados responsáveis pelo tratamento, público ou privados. Essas entidades, impulsionadas pelas necessidades atreladas ao tratamento automatizado de dados, vêm acumulando uma grande quanti-

---

64 Fichas técnicas sobre a União Europeia – 2021. Disponível em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf . [Consulta em 01.02.2021].

65 Bruno Ricardo Bioni, *Op. Cit.*, p. 122.

66 Artigo 8.º

Proteção de dados pessoais

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

67 Artigo 16.º (ex-artigo 286.o TCE)

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.o do Tratado da União Europeia.

dade de informações a ponto de superar o conhecimento que o próprio indivíduo detém sobre ele mesmo. O RGPD surge, assim, em resposta a essa realidade já existente, colocando os dados pessoais e seu tratamento no centro do debate jurídico e empresarial[68].

No contexto do RGPD, a proteção de dados pessoais ostenta *dupla função* por garantir a privacidade e os direitos fundamentais do titular e ao mesmo tempo impor a regras de modo a não obstar ao desenvolvimento econômico[69], o que fica evidenciado já nos primeiros considerando do Regulamento como os de número 1 (proteção de dados como direito fundamental), número 2 (introduz o mister económico do Regulamento não desconectado do foco no bem-estar das pessoas) e número 6 (referência ao impacto tecnológico).

3. *IOT*: NOÇÃO E ENQUADRAMENTO JURÍDICO

3.1. O QUE É *IOT*?

O termo *Internet of Things* (ou, em português, Internet das Coisas), doravante *IoT*, é utilizado hoje para referenciar dispositivos com a característica de serem interconectáveis de modo a tornar possível a criação de uma rede formada por "coisas" de naturezas diversas.

Nos primórdios, a internet foi concebida como uma rede entre computadores, fazendo emergir uma nova realidade em que conviviam, paralelamente, dois mundos: o mundo real, onde viviam as pessoas a manipular os mais diversos objetos e equipamentos, e o mundo virtual, formado por computadores ligados entre si. Assim, para "interagir" ou "espelhar" o mundo real, a internet dependia da intervenção humana para coletar dados do mundo real e processá-los com uma finalidade específica.

Já nessa época inicial do desenvolvimento da *internet* se falava da possibilidade da conexão *device-to-device* (D2D), mas foi apenas em 1999 que o termo *Internet of Things* foi criado por Kekin Ashton por ocasião de uma palestra para a Procter & Gamble[70]. Como precursores desse tipo de tecnologia, são citados diversos autores cujo trabalho consistia em estudar a possibilidade de se interconectar dispositivos capazes de interagir entre si sem intervenção humana. Dentre todos, destacamos Mark Wiser, autor do artigo intitulado "*The computer for the 21ts Century*"[71], no qual cunhou o termo "computação ubíqua" para designar a conexão entre dispositivos

---

68 António de Menezes Cordeiro, *Op. Cit.,* p. 29.

69 Bruno Ricardo Bioni, *Op. Cit.,* p. 108.

70 Kevin Ashton, "That 'Internet of Things' Thing", *in RFID Journal*, 2009, disponível em https://www.rfidjournal.com/that-internet-of-things-thing (Consulta em 01.02.2021)

71 Mark Wiser. "The computer for the 21ts Century", *in Scientific American*, n.º 3, Vol. 265, 1991.

de forma "invisível" às pessoas[72]; e Neil Greenfield, ante a publicação, em Janeiro de 1999, do seu livro "*When the Things Start to Think"*.

Já a criação do primeiro dispositivo considerado como *IoT device* é creditado a John Romkey, responsável pela criação de uma torradeira ligada à internet (rede TCP-IP) e controlável através de um computador[73].

Não há, no âmbito europeu uma definição legal para Internet das Coisas, mas há na literatura especializada diversos conceitos propostos[74], sempre mencionando a conectividade entre objetos dos mais variados, por meio de protocolos de comunicação[75]. Para além da característica de interconectividade (D2D), o desenvolvimento tecnológico acrescentou ao mundo da *IoT* outras funcionalidades que potencializaram sua eficiência tais como a conectividade *wireless* (*Bluethooth, wi-fi,* identificação por radiofrequência RFID), a inteligência artificial (sobretudo com a introdução do *machine learning)* e a coleta de dados sem intervenção humana (através da associação dos dispositivos a sensores)[76].A coleta e tratamento desses dados possi-

---

72 Scott R. Peppet, "Freedom of Contract in Augmented Reality", *in Research Handbook on the Law of Virtual and Augmented Reality*. Chelteham, Edward Elgar, 2020, p. 609.

73 O dispositivo, depois melhorado para incorporar um robô responsável por introduzir o pão, foi apresentado na Interop 89' Conference com a inovação de ser 100% automatizado por funcionar sem qualquer interação humana.

74 Por exemplo, para Ken Goldstein , "*IoT is the concept for connecting a device to the Internet and other connected devices*." Ken Goldstein, "Cyber Beware: Iot Technology Growing Explosively.", *in International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel*, n.º 6, Vol. 3, 2019, disponível em https://heinonline.org/HOL/P?h=hein.journals/idpp3&i=131 (Consulta em 01.08.2021). Já para Noto La Diega, *IoT* "*entails any physical entity capable of connectivity that directly interfaces the physical world, such as embeddes devices, sensors and actuators*". Noto La Diega, "Internet of things and patents: Towards the iot patent wars.", *in Journal of Commercial and Intellectual Property Law*, n.º 2, Vol. 3, 2017, disponível em https://heinonline.org/HOL/Page?handle=hein.journals/tfm2017&id=223&collection=journals&index= (Consulta em 01.08.2021). Elvy, vai além da conectividade e menciona *"a network of products, systems and platforms connected through enable devices that collect, store and communicate with other devices, cloud software, on-site infrastructure, and individuals to maximize efficiency*". Stacy-Ann Elvy, "Contracting in the age of the internet of things: article of the ucc and beyond.", *in Hofstra Law Review*, nº 3, Vol. 44, 2016, disponível em https://heinonline.org/HOL/Page?public=true&handle=hein.journals/hoflr44&div=40&start_page=839&collection=-journals&set_as_cursor=0&men_tab=srchresults (Consulta em 01.08.2021)

75 Larisa-Antonia Capisizu, "Legal Perspectives on the Internet of Things", *in Conferinta Internationala de Drept, Studii Europene si Relatii Internationale*, 2018, disponível em https://heinonline.org/HOL/Page?public=true&handle=hein.journals/cidstue2018&div=55&start_page=523&collection=journals&set_as_cursor=0&men_tab=srchresults (Consulta em 08.08.2021)

76 Nos dias atuais, a torradeira de Romkey, para além de ser acionável por um comando de computador ou *smartphone* a ela conectados através de rede sem fio, poderia ser interligada aos dados da agenda eletrônica de seu usuário e iniciar a operação de modo sincronizado ao horário do alarme que o desperta. Ainda, a torradeira seria capaz de guardar informações acerca do comportamento do utilizador, como a hora em que ele efetivamente

bilitam ao dispositivo mapear o comportamento do utilizador de modo a proporcionar uma experiência inteiramente personalizada.

Tais características da tecnologia *IoT* torna-a penetrável em todos os ambientes e aspetos da vida cotidiana, já que os chamados dispositivos inteligentes (*smart device*) tomam as mais diversas formas, desde automação doméstica (domótica), passando por roupas e acessórios (*wearables),* brinquedos (*smart toys*), até grandes máquinas industriais, cidades inteligentes (*smart cities*) e equipamentos de mobilidade (*smart cars*). Concretizado, assim, o caráter da ubiquidade computacional previsto Mark Wiser no início da década de 1990.

A partir de então, a realidade do mundo assume um formato no qual o ambiente físico se confunde com o digital[77]. Agora, não é mais necessária a intervenção humana para fornecer dados da realidade física para os computadores, pois os diversos dispositivos do nosso dia-a-dia são dotados de sensores e coletam esses dados automaticamente, bem como compartilham esses dados com outros dispositivos, possibilitando o cruzamento de informação e a confecção de perfis comportamentais cada vez mais precisos.

Por esse motivo, não teria sido possível o desenvolvimento da *IoT* não fosse a realidade do *Big Data*[78]. A revolução do *Big Data* tornou-se possível em razão, dentre outros fatores, da redução do preço do silicone, do barateamento das tecnologias de conectividade e do *Cloud Computing*, essencial para ao aumento da capacidade de armazenamento. Conforme ensina Ugo Pagallo, Massimo Durante, e Shara Monteleone[79] a *computação em nuvem* condensou em si as vantagens do fácil acesso com o armazenamento extenso e barato, características potencializadas pela conexão 5G, as interconexões via radio e outras redes invisíveis e a ubiquidade da telefonia móvel

Tamanha facilidade não viria sem ônus. Hoje, é crescente o debate acerca da banalização dos dispositivos hiperconectados com benefícios questionáveis, fazendo surgir o termo *internet das coisas inúteis.* Sobre isso, ensina

recolhe a torrada para consumo e em que situações ele precisa reaquecer o alimento por ter, por exemplo, sido preparado demasiado cedo.

77 Ilustra essa nova realidade o *slogan* difundido por executivos da Google segundo o qual agora "*We don´t go online. We live online*" em referência ao contraste entre o mundo cibernético atual, no qual vivemos hiperconectados, e aquele experimentado outrora, quando selecionávamos momentos do dia para "acessar" a internet.

78 A definição primeira de *Big Data* é atribuída a Doug Laney que inaugurou a famosa referência aos 3V's relativos ao volume de dados, velocidade de processamento e variedade de análises. Mais tarde foram acrescentados mais dois V´s referentes a veracidade e valor, conforme narra Ugo Pagallo, "The legal challenges of big data: Putting secondary rules first in the field of eu data protection", *in European Data Protection Law Review (EDPL)*, n.º 1, Vol. 3, 2017. pp.36-46.

79 Ugo Pagallo, Durante Massimo e Shara Monteleone, "Whats is New with the Internet of Things in Privacy and Data Protection For Legal Chalenges on Sharing and Control in IoT.", *in Data Protection and Privacy: (In)visibilities and Infrastructures,* Ronald Leenes, *et al*. Cham, Springer, 2017. (Law, governance and technology series). pp. 59-78.

Magrani[80] que o barateamento e popularização dessa tecnologia permitiu a associação da avançada tecnologia a objetos triviais, sem utilidade proporcional. Assim, sob a promessa de facilitar a vida, a tecnologia pode influir apenas para complicar o uso e encarecer o produto sem contrapartida significativa[81].

A ameaça potencial da *IoT* que mais interessa ao presente trabalho, todavia, relaciona-se com os perigos envolvendo a segurança da informação e a proteção de dados. Isso porque, cada dispositivo, por mais simples ou pouco útil, representa uma porta de coleta dados, dados esses que serão somados às inúmeras informações coletadas pelos diversos dispositivos conectados a uma mesma rede. Esse volumoso conjunto de dados (*big data*) permite traçar um perfil cada vez mais preciso do indivíduo, mapeando e prevendo seus hábitos, preferência e escolhas e dando às máquinas – e consequentemente às empresas e pessoas que as controlam – o poder de conhecer o usuário mais do que ele mesmo[82].

A grande preocupação, nesse contexto, é o poder garantido pelas empresas detentoras dos dados e terceiros que compram seus produtos, pois as estratégias de *marketing* crescem exponencialmente em efetividade e tornam-se capazes de manipular silenciosamente as mentes e induzir escolhas de consumo[83]. A propaganda detalhadamente personalizada e com alvo minunciosamente definido deixa de exercer o tradicional efeito meramente persuasivo e passa a funcionar como um controlo da própria vontade individual, dando ensejo a verdadeira "ditadura dos dados"[84]. Para além disso, a rapidez com que esses dispositivos penetraram nossa vida cotidiana e o baixo grau de informação disponível aos usuários resulta em um consumo irrefletido desses produtos, pois os usuários pouco se preocupam com o local e grau de segurança do armazenamento desses dados, ou com a destinação e uso desses dados pela entidade deles detentora.

---

80 Eduardo Magrani, *A Internet das Coisas,* Rio de janeiro, FGV Editora, 2018.

81 Como exemplo, Magrani cita o produto *egg minder* consistente em uma bandeja com sensor para contabilizar o número de ovos em determinado frigorífico, destacando a preocupação com a sustentabilidade ambiental, pois os dispositivos inúteis possuem a tendência de tornarem-se rapidamente ultrapassados e serem descartados, gerando grande volume de lixo tóxico para o qual não há destinação (*e-waste*). Eduardo Magrani *, Op. Cit.*, p. 222.

82 Hélder Frias, "A Internet de Coisas (IoT) e o Mercado Segurador.", *in FinTech: desafios da tecnologia financeira.* coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte. Vol. 1. Almedina, Coimbra, 2017. pp. 219-233.

83 Madalena Perestrelo de Oliveira, "Definição de Perfis e Decisões Automatizadas no Regulamento Geral sobre a Proteção de Dados.", *in FinTech: desafios da tecnologia financeira.* coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte, Vol. 2, Almedina, Coimbra, 2017. pp. 61-88.

84 Bruno Ricardo Bioni, *Op. Cit.*, pp. 89-92, para quem "no contexto do *Big Data*, são os algoritmos que passam a orquestrar as dessas pessoas, decidindo a respeito das suas oportunidades."

Sobre o assunto, explica Siegel[85] que a maioria dos consumidores utilizam os dispositivos inteligentes com o objetivo de facilitar e simplificar suas rotinas quotidianas, sem considerarem ou sequer terem conhecimento do grau de segurança desses aparelhos em relação aos seus dados. Para além do risco de invasões de privacidade por meio de *hackers* com o objetivo de controlar o próprio dispositivo (que pode ser desde um simples sensor de presença a um brinquedo inteligente dotado de câmera e poder de interação com a criança), falhas de segurança também podem permitir um ataque *hacker* atraído pela volumosa quantidade de dados coletados. Alerta ainda o autor que, mesmo sendo cada vez mais regulares e frequentes as invasões e os vazamentos de informações, as pessoas parecem não levar a sério os riscos ou, quando os consideram, não sabem como se proteger deles.

Essas preocupações embora se refiram à toda gama de inovações tecnológicas, apresenta-se mais acentuada no caso dos dispositivos *IoT* ante penetrabilidade desse tipo de tecnologia nos aspetos mais íntimos da vida humana. Por exemplo, mesmo se tomarmos como parâmetro o impacto das redes sociais da esfera da privacidade – tendo em conta que o arranjo social estimula que os indivíduos compartilhem com o grande público toda a sorte de informações pessoais que obviamente os expõem – esse impacto ainda é consideravelmente menor do que o proveniente da Internet das Coisas.

Em sua maioria, os dados coletados no âmbito das redes sociais são controlados pelos seus usuários ao selecionarem que fotos compartilham, quais dados introduzem em seus perfis e quais pessoas têm acesso àquelas informações. Já no campo da *IoT*, os dispositivos, por exemplo, componentes de uma rede doméstica, estão silenciosamente absorvendo todos os dados daquele núcleo familiar (ubiquidade), desde o número de pessoas, seus hábitos, conversas, perfil de consumo, preferências musicais e outros aspetos de comportamento dos mais triviais aos mais íntimos.

Um exemplo desse comparativo, envolvendo uma espécie de dados especialmente sensíveis e íntimos, são os casos envolvendo redes sociais de relacionamento. Vazamento de informações coletadas por aplicações como o *Tinder*[86] ou no famoso caso *Ashley Madison*[87] têm o potencial, como é óbvio, de expor os usuários à humilhação pública e à devassa da intimidade. Mas é

---

85 Jeremy Siegel, "When the Internet of Things Flounders: Looking into GDPR-Esque Security Standards for IoT Devices in the United States from the Consumers' Perspective.", *in Journal of High Technology Law*, n.º 1, Vol. 20, 2020, pp. 189-229, disponível em https://heinonline.org/HOL/Page?handle=hein.journals/jhtl20&id=189&collection=journals&index= (Consulta em 01.04.2020)

86 A aplicação de relacionamento mais famosa do mundo.

87 *Site* destinado às pessoas que procuram relacionamentos extraconjugais, cujos dados foram vazados em 2015, expondo estimados 33 milhões de usuários, conforme amplamente noticiado pela mídia. Notícia Disponível em <https://www.publico.pt/2015/08/21/tecnologia/noticia/portugueses-estao-no-ashley-madison-a-maioria-no-norte-do-pais-1705602>, (Consulta em 30.6.2020)

de se admitir que o grau de detalhe das informações lançadas à plataforma é controlado pelos participantes (escolha de fotos e informações pessoais publicadas ou conteúdo das conversas estabelecidas).

Por outro lado, é inegavelmente mais agressiva a exposição sofrida pelos consumidores no caso, também amplamente divulgado[88], envolvendo o *smart sex toy* manufaturado pela empresa canadiana *We-Vibe*. Nesse caso, consumidores americanos acionaram judicialmente a fabricante de um vibrador, cujo diferencial era o de ser controlável por meio de aplicação no telemóvel. Descobriu-se, entretanto, que o dispositivo coletava, sem consentimento específico, dados pessoais sensíveis dos utilizadores tais como data, duração e configuração de cada utilização, reportando, em tempo real, ao fabricante.

Note-se que, nesses casos, até mesmo as tentativas de anonimização dos dados são por vezes mal sucedidas, pois o volume e qualidade dos dados, mesmo que dissociados de uma identificação nominal, possibilitam a individualização do titular e garantem a reversibilidade do processo de anonimização. Segundo analisa Brasher, a avançada tecnologia da Internet das Coisas permite análises impossíveis em um cenário com quantidade reduzida de dados; a esse fator soma-se a ampla possibilidade de compartilhamento desses dados, de cruzamento de informações colhidas por dispositivos distintos e a coleta de dados sensíveis indistintamente. Tudo isso, resulta não só numa coleta de dados mais intrusiva, mas no aumento do risco de reversão do processo anonimização[89].

A violação da privacidade dos consumidores, nesse caso, alcançava potencialmente dados de que os titulares sequer tinham controlo ou conhecimento. Mais ainda, mesmo que ao comprar o dispositivo *smart* o indivíduo médio antecipe a ocorrência da coleta e tratamento de dados pessoais, não tem como prever exatamente quais são esses dados e nem o tipo ou finalidade do tratamento, realizado em sua quase totalidade sem interferência humana. Essa é, notadamente, a circunstância que justifica a acentuada preocupação quando se trata de proteção de dados e da privacidade do usuário de dispositivos *IoT* quando comparado a outras modalidades de coleta.

Outro ponto essencial para estabelecermos os contornos do problema, é a penetrabilidade da coleta de dados decorrente do crescimento exponencial, quase generalizado, do uso de *smartphones*. Isso porque, ao contrário dos objetos inteligentes – ao alcance apenas de uma parcela da população –, os *smartphones* representam a evolução dos telemóveis comuns e, por sua

---

88 Conforme notícia do *The Guardian* disponível em https://www.theguardian.com/technology/2017/mar/14/we-vibe-vibrator-tracking-users-sexual-habits e no portal português "Sábado", disponível em https://www.sabado.pt/ciencia---saude/detalhe/fabricante-de-vibradores-condenado-por-espiar-utilizadoras (Consulta em 30.6.2020)

89 Elizabeth A. Brasher, "Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation.", *in Columbia Business Law Review*, n.º 1, 2018, pp. 209-253, disponível em https://heinonline.org/HOL/Page?handle=hein.journals/colb2018&id=215&collection=journals&index=# (Consulta em 01.08.2021)

vez, dos telefones domésticos, cuja utilização já se encontra há anos sedimentada nos costumes. Por isso, é reduzido o público alheio à revolução do *Big Data*, dando ensejo a um fenômeno nomeado *datificação das vidas*[90].

O fenômeno representa a transformação da vida do indivíduo em um apanhado de dados contendo todas as *nuances* de sua existência, significando não só o seu rastreio virtual (histórico de navegação na internet, por exemplo) mas a sua localização física constante também no mundo *offline* (sociedade da vigilância). A base disso, segundo Solove, está na elaboração de verdadeiros *dossiês digitais* utilizados pelas empresas para descobrir novas formas de fazer negócios, pelo mercado financeiro para determinar a quem aprovará crédito, pelos empregadores para analisar o passado de candidatos a empregos, pelos órgãos governamentais para investigar cidadãos e descobrir roubos e fraudes e outros usos ainda não conhecidos [91].

Esses dossiês electrónicos funcionam, assim, como um prolongamento digital do indivíduo e, para além de sua representação em formato de *bits*, há a classificação e segmentação das pessoas com base em tais informações, em uma atividade denominada *profiling*[92]: prática que agrupa os dados pessoais de um indivíduo de modo a elaborar um relatório a seu respeito a fim de basear a tomada de inúmeras decisões. Tais perfis permitirão a classificação da pessoa de acordo com determinados estereótipos e servirão de filtro invisível para o direcionamento de conteúdos disponíveis na rede.

A técnica da definição de perfis (*profiling*), no caso da Internet das Coisas, pode, então, ser desmembrada em três elementos: a coleta dos dados (efetuada diretamente pelo dispositivo por meio de sensores, fornecida por terceiros ou disponíveis na *nuvem*); o tratamento automatizado por meio de um algoritmo (*machine learning*); e a decisão automatizada (*decision making*)[93]. Os dados coletados, frise-se, são utilizados não só para compor o perfil do titular a ele correspondente, mas também servem como substrato para a definição de padrões de comportamento (necessários para categorização dos demais perfis) e como espécie de guia para checagem das decisões automatizadas a cada processamento, de modo que o ciclo se retroalimenta[94].

A preocupação surge da potencialidade de doutrinar-se a pessoa com um conteúdo e uma informação ditados pelos interesses inferidos por intermédio dos seus dados, isolando-a da interação com conteúdos diferentes que

---

90 Bruno Ricardo Bioni, *Op. Cit.,* pp. 87/88.

91 Daniel J. Solove, *The Digital Person*, New York and London, New York University Press, 2004.

92 Bruno Ricardo Bioni, *Op. Cit.,* pp. 89 e ss.

93 , Dimitra Kamarinou, Christopher Millard e Jatinder Singh, "Machine Learning with Personal Data", *in Data Protection and Privacy: The Age pf Intelligent Machines,* Ronald Leenes, *et al*. Oxford, Hart, 2017, pp. 89-112.

94 Dimitra Kamarinou, Christopher Millard e Jatinder Singh, *Op. Cit.*

fogem ao perfil enquadrado, com influência nos mais variados aspetos da vida desde a celebração de contratos até o acesso à informação[95].

Todas essas características e peculiaridades têm preponderante impacto na análise do direito à proteção de dados pessoais e da aplicação do RGPD em relação aos dispositivos de Internet da Coisas por suscitarem problemas e discussões não existentes em relação a outros universos abrangidos pela proteção de dados.

3.2. APLICABILIDADE DO RGPD AOS DISPOSITIVOS IOT

Sob a perspectiva da aplicabilidade material do RGPD, o artigo 2.º do Regulamento estabelece ser aplicável as suas regras "*ao tratamento de dados pessoais por meios total ou parcialmente automatizados*", com exceção das hipóteses elencadas no próprio artigo. Não há dúvidas que, nesse aspeto, as operações desempenhadas pelos dispositivos de *IoT* estão abarcadas pela aplicação material do Regulamento sempre que se referirem a dados pessoais, sobretudo em razão da amplitude desse conceito trazido pelo RGPD no artigo 4.º.

Em relação à aplicação territorial, o artigo 3.º do RGPD estabelece dois critérios de aferição, quais sejam o critério do *estabelecimento* (n.º 1) e o do *direcionamento* (n.º 2).

De acordo com o primeiro critério, incidirá o RGPD sempre que o tratamento de dados pessoais for efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento. Nesse quesito, uma primeira observação acerca dos dispositivos de *IoT* é a de que a atividade de tratamento será total ou parcialmente desenvolvida pelo próprio dispositivo, sem que esse tratamento se vincule a nenhum estabelecimento comercial, seja do fabricante/desenvolvedor do aparelho, seja do vendedor. Logo, a aplicabilidade do Regulamento pode ser questionada, sob o critério do estabelecimento (artigo 3.º, n.º 1), nas hipóteses em que o dispositivo é comprado em estabelecimento estrangeiro e também foi fabricado por empresa sem estabelecimento na União Europeia.

Também é importante sopesar o contexto atual de desenvolvimento tecnológico e a realidade de já existirem empresas sem estabelecimentos físicos e com atuação global. Não raras são as empresas não localizadas em lugar nenhum a não ser no meio virtual. Nesse aspecto, é indiferente, nos termos do próprio regulamento, o local onde estão armazenados os dados coletados (servidor) ou onde ocorre a atividade de tratamento em si, se dentro ou fora dos limites da União. Além disso, a localização dos titulares dos dados, por esse critério, não é tomada em consideração para fins de aplicação do RGPD. Ou seja, na hipótese de tratamento realizado no con-

95 Bruno Ricardo Bioni, *Op. Cit., p. 91*

texto de um estabelecimento situado em qualquer dos Estados-Membros[96], o Regulamento será aplicável mesmo que se refiram a pessoas singulares localizadas fora do território da União[97].

Igualmente irrelevante, para fins de avaliar o local do estabelecimento, é o critério formal de registo empresarial, pois o considerando 22 do RGPD expressamente dispõe que "*estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável*.", não sendo fator determinante a sua forma jurídica. O texto do considerando vai, outrossim, ao encontro da disposição já existente na revogada Diretiva 95/46/CE e também do teor da jurisprudência do TJUE[98] nos casos *Google Spain* contra AEPD[99], *Weltimmo* contra a NAIH[100] e VKI (Associação de proteção dos consumidores austríaca) contra *Amazon EU Sàrl*[101].

Para o Comité Europeu de Proteção de Dados, a interpretação, a ser realizada caso a caso, não pode ser restritiva, sob pena de não se alcançar o objetivo de garantir uma proteção eficaz e completa. Por outro lado, não se pode exceder na amplitude interpretativa de modo a permitir a conclusão de que qualquer presença na UE é suficiente para atrair a incidência da legislação da UE em matéria de proteção de dados[102].

Já o artigo 3.º, n.º 2 do RGPD, estabelece o critério do *direcionamento* para fins de análise da aplicação territorial do Regulamento, de modo que a

---

96 COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD) Diretrizes 3/2018 sobre o âmbito de aplicação territorial do RGPD (artigo 3.º), versão 2.0, de 12.11.2019, disponível em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf (Consulta em 01.08.2021) No documento, o CEPD apresenta o seguinte exemplo: uma empresa francesa desenvolveu uma aplicação de partilha de automóveis exclusivamente destinada a clientes de Marrocos, da Argélia e da Tunísia. O serviço apenas está disponível nesses três países, mas todas as atividades de tratamento de dados pessoais são efetuadas em França pelo responsável pelo tratamento de dados. Nesse caso, é aplicável o RGPD, nos termos do artigo 3.º, nº 1.

97 Nesse sentido, destaca-se o teor do considerando 14: A proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais.

98 Embora todos esses precedentes remetam à época anterior à vigência do RGPD, entendemos, no mesmo sentido de CEPD, que são relevantes para fins de interpretação da regra do artigo 3.º, n.º 1, notadamente da expressão "tratamento no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou subcontratante". COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). *Op. Cit.,* p. 8.

99 Caso *Google Spain* contra AEPD (C-230/14, EU:C:2014:317). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62012CJ0131&from=PT (Consulta em 28.7.2021)

100 Caso *Weltimmo* contra NAIH (C-230/14, EU:C:2015:639). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62014CJ0230&qid=1625334800153&from=PT [Consulta em Julho de 2021]

101 Caso VKI (*Verein für Konsumenteninformation*) contra *Amazon EU Sàrl* (C-191/15, EU:C:2016:612).

102 COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). *Op. Cit.* p. 8.

ausência de estabelecimento empresarial do responsável pelo tratamento em um dos Estados-Membros não é suficiente de *per si* para afastar a incidência do Regulamento. Do texto do dispositivo legal extrai-se duas novas hipóteses de aplicação territorial, sendo irrelevante o facto de existir ou não estabelecimento do responsável pelo tratamento na União Europeia, desde que, em qualquer dos dois casos, se refira ao tratamento de dados pertencentes a titulares que se encontrem na União Europeia, não sendo necessário que se trate de nacional de algum Estado-membro, sequer residente. Todavia, para o CEPD, o dispositivo deve ser interpretado no sentido de se considerar as atividades dirigidas intencionalmente, e não de modo inadvertido ou acidental, a indivíduos situados na UE[103].

Para além de se encontrar o titular na União Europeia, para ser aplicável o RGPD, é preciso ainda que se configure umas das hipóteses descritas nas alíneas *a)* e *b)* do dispositivo, ou seja, *oferta de bens ou serviços* na União Europeia[104] ou *controlo de comportamento de pessoas* localizadas na União Europeia.

Na primeira hipótese, o aplicador do direito deverá considerar todos os elementos fáticos (moeda utilizada na transação, língua, área de entrega de mercadoria, menção a especificidades voltadas ao público europeu, etc.) a fim de definir se, em conjunto, demonstram *evidente intenção* do responsável de ofertar produto ou serviço ao público europeu, mesmo não estando estabelecido em nenhum dos Estados-membros. Saliente-se, ainda, que a análise não tem por objetivo definir, de modo estanque, se o RGPD se aplica ou não a uma empresa, na condição de responsável pelo tratamento de dados, mas se se aplica a uma determinada operação. Assim, um mesmo responsável pelo tratamento (ou subcontratante) pode, ao mesmo tempo, estar vinculado às regras do RGPD em relação a parte de suas atividades, e não estar em relação a outra parte[105].

Na segunda hipótese (artigo 3.º, n.º 2, *b)*), há uma infinidade de situações possíveis relacionadas a tratamento de dados por meio de dispositivos *IoT*, pois tais aparelhos têm como principal atividade justamente a coleta de dados relativos a comportamento, com definição de perfis e tomada de decisões automatizadas e personalizadas[106]. O CEPD, inclusive, faz menção

---

103 COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). Op. Cit. p. 17.

104 O considerando 23 do RGPD esclarece ter que ser "evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União."

105 COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). *Op. Cit.* pp. 21/22, onde consta o exemplo de uma universidade que oferece vagas em cursos voltados ora para público nacional e ora para a comunidade académica internacional. Apenas em relação a esse último caso será aplicável o Regulamento, especificamente em relação aos dados por ventura sejam coletados no processo seletivo cujo público-alvo envolvia intencionalmente pessoas localizadas na UE.

106 Madalena Perestrelo de Oliveira, "Definição de Perfis e Decisões Automatizadas no Regulamento Geral sobre a Proteção de Dados." *in FinTech: desafios da tecnologia financeira.* coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte, Vol. 2. Almedina, Coimbra, 2017. pp. 61-88.

a essa particularidade nas Diretrizes 3/2018[107] ao se referir ao considerando 24[108] do RGPD e esclarecer considerar aplicável a mesma regra a outros tipos de controlo de comportamento por meio de aparelhos usáveis (*wearable*) e outros dispositivos inteligentes. Por fim, o Comité elenca exemplificativamente atividades que considera configurar controlo, entre as quais, publicidade comportamental, atividades de geolocalização e controlo do estado de saúde de uma pessoa[109].

Também é importante salientar que o responsável pela atividade de tratamento pode subcontratar empresas para executar operações em seu nome e sob suas instruções, sem que isso afaste a aplicação do Regulamento, independentemente de o subcontratante possuir ou não estabelecimento na União Europeia. Ademais, nos termos do artigo 27.º, nas hipóteses de aplicação do RGPD, por força do artigo 3.º, n.º 2, deverá o responsável pelo tratamento ou o subcontratante designar por escrito um representante, sem que isso configure "estabelecimento"[110].

Pelo exposto, extrai-se dos termos do RGPD que suas regras serão aplicáveis a operações de tratamento realizadas através de dispositivos de *IoT* tanto quanto a qualquer outra operação de tratamento, desde que observadas as hipóteses legais. Porém, não se pode negar que algumas particularidades da *IoT* trazem específicos desafios quando da avaliação da incidência do Regulamento, notadamente em razão do fato de a atividade de tratamento ser, em boa parte, executada por máquinas, sem qualquer intervenção humana, bem como de haver interligação, com compartilhamento de dados, entre os mais variados sistemas e dispositivos, dificultando muitas vezes a identificação do "responsável" pelo tratamento[111]. Por isso, ressalta-se ainda mais a importância do atendimento, pelas empresas componentes da cadeia de produção e distribuição dos dispositivos, ao princípio da trans-

---

107 COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). *Op. Cit*. p. 22.

108 Considerando 24: O tratamento de dados pessoais de titulares de dados que se encontrem na União por um responsável ou subcontratante que não esteja estabelecido na União deverá ser também abrangido pelo presente regulamento quando esteja relacionado com o controlo do comportamento dos referidos titulares de dados, na medida em que o seu comportamento tenha lugar na União. A fim de determinar se uma atividade de tratamento pode ser considerada «controlo do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes.

109 COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). *Op. Cit.* p. 23.

110 COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). *Op. Cit*. p. 27.

111 Essa dificuldade já foi destacada pelo Comité Europeu, mas no âmbito da responsabilidade civil: COMITÉ ECONÓMICO E SOCIAL EUROPEU Parecer sobre «Confiança, privacidade e segurança para os consumidores e as empresas na Internet das coisas (IdC)» Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018IE1038&qid=1625339548895&from=PT (Consulta em 01.07.2021) itens 3.1 e 3.4.

parência e a informação as entidades direta ou indiretamente envolvidas no processo de tratamento[112].

4. PRINCIPAIS DESAFIOS DO RGPD FRENTE ÀS INOVAÇÕES TECNOLÓGICAS DA IOT

4.1. OBJETIVOS E PRINCÍPIOS DO RGPD

O desenvolvimento da chamada "Era da informação" somado aos objetivos da União Europeia, notadamente ante a livre circulação de produtos e pessoas resultou na idealização do Mercado Único Digital, com a construção de um ambiente digital livre e seguro no âmbito da União Europeia. É nesse contexto que o RGPD surge, em substituição da Diretiva 95/46/CE, mormente da necessidade de um complexo normativo que garanta a proteção adequada e idêntica dos dados pessoais nos Estados da UE e a circulação da informação no âmbito europeu[113].

Assim, pode-se dizer que a espinha dorsal do RGPD é constituída de dois grandes objetivos: para além de proteger direitos fundamentais das pessoas singulares, notadamente o direito à proteção de dados, o Regulamento tem por objetivo promover a livre circulação dos dados pessoais. O RGPD, portanto, não se propõe a impedir o tratamento de dados pessoais. Ao contrário, o mister o Regulamento ratifica a licitude desse tratamento e estabelece as bases legais para que a atividade se dê em benefício do desenvolvimento econômico e tecnológico, sem pôr em xeque, todavia, a privacidade e demais direitos dos titulares[114].

Digno de realce é a abrangência material do RGPD. Apesar da associação imediata do Regulamento ao desenvolvimento tecnológico e ao mundo digital, suas regras se aplicam igualmente aos dados constantes de documentos físicos e tratados de modo não digital. Esse grande alcance do RGPD exige do intérprete e do aplicador do direito uma leitura dos princípios e conceitos da lei sob diferentes perspectivas, tendo sempre em consideração a natureza do tratamento de dados. Do contrário, uma leitura anacrónica dos dispositivos legais pode servir de equivocado entrave aos avanços tecnológicos.

---

112 A maior atenção ao princípio da transparência em relação aos dispositivos de *IoT* foi destacada pelo GT29 desde a Opinião n.º 8/2014. GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Opinion 8/2014 on the on Recent Developments on the Internet of Things.* Setembro, 2014. Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (Consulta em 01.07.2021)

113 Alexandre Sousa Pinheiro, et al. Comentário ao regulamento geral de proteção de dados. Almedina, 2018, p. 97.

114 António de Menezes Cordeiro, *Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019.* Coimbra, Almedina, 2020, p. 33.

Em relação aos princípios do tratamento de dados, são listados no artigo 5.º do RGPD: *licitude, lealdade e transparência* (n.º 1, *a)*); *limitação das finalidades* (n.º 1, *b)*); *minimização dos dados* (n.º 1, *c)*); *exatidão* (n.º 1, *d)*); *limitação da conservação* (n.º 1, *e)*); *integridade e confidencialidade* (n.º 1, *f)*) e *responsabilidade* (n.º 2).

A licitude deve ser entendida na sua acessão estrita, ou seja, não apenas deve estar de acordo com as leis, de uma forma geral, mas o princípio indica uma necessidade de o tratamento de dados corresponder a uma das hipóteses enumeradas no artigo 6.º do Regulamento[115]. Tal interpretação é extraída da própria redação legal, pois o artigo 6.º estabelece ser apenas lícito o tratamento enquadrado em alguma daquelas situações.

Por sua vez, o princípio da lealdade reforça a proteção do titular de dados ao impedir que o tratamento ocorra em seu prejuízo mesmo em situações potencialmente consideradas como lícitas. O termo, contudo, trata de um conceito aberto e, portanto, pouco preciso, sobretudo consideradas as lacunas vocabulares entre as diferentes línguas[116]. Assim, o atendimento do princípio da lealdade deverá ser observado em concreto, caso a caso, considerada a relação entre o responsável pelo tratamento e o titular, bem como suas legítimas expectativas.

O princípio da transparência representa importante pilar do RGPD, não só por constituir uma das novidades do diploma em relação à Diretiva 95/46/CE[117], mas também por ser relevante tê-lo em consideração, para fins de legitimidade do tratamento, durante todo o processo de tratamento. Isso porque, além das informações a serem prestadas no momento da recolha (artigo 13.º, ns.º 1 e 2), o dever de transparência determina que o titular continue a ser informado, por exemplo, em relação ao tratamento posterior dos dados pessoais (artigo 13.º, n.º, 3). É esse princípio, também, a base para o direito de acesso aos dados (artigo 15.º, n.º 1).

Ademais, não basta apenas prestar as informações, sendo imprescindível que elas sejam prestadas de forma concisa e acessível, com linguagem clara e simples. Ou seja, o responsável pelo tratamento deve envidar todos os esforços para estabelecer uma efetiva comunicação com o titular e deixá-lo ciente de todo o processo de tratamento, de seus direitos e das medidas de segurança adotadas.

Já o artigo 5.º, n.º 1, *b)* condiciona a recolha de dados à existência de uma finalidade *determinada*, *explícita* e *legítima*, em congruência com o artigo 8.º, n.º 2 da Carta Dos Direitos Fundamentais da União Europeia. Para o Grupo de

---

115 António de Menezes Cordeiro*, Op. Cit.*, p. 152.

116 António de Menezes Cordeiro*, Op. Cit*., p. 153. Conforme descreve o autor, o princípio aparece na versão italiana do Regulamento como *correttézza,* na inglesa, como *fairness* e, na alemã, como *Treu und Glauben*, as quais não correspondem propriamente à tradução de lealdade, presente nas versões em português, espanhol e francês.

117 António de Menezes Cordeiro*, Op. Cit.*, p. 154.

Trabalho do Artigo 29.º para a Proteção de Dados (GT29)[118] a exigência dos fins específicos é essencial para a análise do grau de interferência razoável na esfera privada do titular[119] e também representa uma salvaguarda à autodeterminação informacional a medida que é essencial para a garantia do controlo dos dados pelo titular[120]. Note-se que não há impedimento à existência de múltiplas finalidades, porém elas devem ser previamente conhecidas pelo responsável pelo tratamento e informadas ao titular (explícitas), além de respeitar, cada uma delas, as exigências legais (legítimas).

A segunda parte do dispositivo também permite que seja estabelecida uma nova finalidade no curso do processo de tratamento, desde que "não incompatíveis" com a finalidade originária. Nesse quesito, ensina Barreto Menezes Cordeiro[121] que, na análise dessa "não incompatibilidade" devem ser observados os fatores enumerados no artigo 6.º, n.º 4 do RGPD, devendo o responsável, também, certificar-se do respeito pelos princípios em relação às novas finalidades, bem como informar o titular dessa decisão (artigos 13.º, n.º 3 e 14.º, n.º 4).

Também como forma de reduzir a coleta dos dados apenas ao necessário, o RGPD estabelece o princípio da minimização (artigo 5.º, n.º 1, *c)*). Pelo princípio, não basta a mera apresentação de uma finalidade legítima, sendo essencial também que essa coleta se resuma ao mínimo necessário. Ficam excluídos, assim, os dados não relacionados com a finalidade, os inapropriados e os dispensáveis, sobretudo quando é possível atingir o fim almejado com o suporte de técnicas menos invasivas, como a anonimização e a pseudonomização.

O princípio da exatidão é autoexplicativo e exige que os dados mantidos sejam corretos e, além disso, atualizados sempre que necessário. Consequentemente, é dever do responsável pelo tratamento apagar ou retificar dados incorretos ou desatualizados.

Já o artigo 5.º, n.º 1, *e)* estabelece uma limitação temporal, ao determinar caber ao responsável pelo tratamento definir e informar ao titular a periodicidade para apagamento e atualização dos dados. O princípio visa obstar à manutenção das informações por tempo excessivo, expondo seus titulares desnecessária e/ou permanentemente.

---

118 O GT29 é o grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018, quando teve seus documentos ratificados na primeira seção plenária do Comité Europeu para a proteção de Dados, conforme informação disponível em https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en [Consulta em Setembro de 2021]

119 GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Opinion 3/2013 on purpose limitation.* Abril, 2013. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (Consulta em 01.07.2021)

120 António de Menezes Cordeiro*, Op. Cit*., p. 155.

121 António de Menezes Cordeiro*, Op. Cit*., p. 157.

A última alínea do artigo 5.º, n.º 1 estabelece os princípios da integridade e confidencialidade com o fim de reforçar a responsabilidade do detentor dos dados em relação à segurança da informação propriamente dita.

Por fim, o princípio de responsabilização, trazido pelo artigo 5.º, n.º 2 funciona como norma de efetivação das anteriores ao definir não apenas o dever do responsável pelo tratamento de agir em conformidade com os princípios, mas também a responsabilidade de comprovar essa conformidade.

4.2. OS CONCEITOS DO RGPD SOB A PERSPECTIVA TECNOLÓGICA DA IOT

Como dito, o RGPD se propõe a normatizar as diversas modalidades de tratamento de dados, equilibrando a tensão aparentemente existente entre o valor dos dados pessoais na sociedade da informação e a imprescindível proteção dos direitos fundamentais e da esfera privada do indivíduo. Por isso, cabe ao intérprete da lei analisar os conceitos gerais e as diversas regras impostas no Regulamento considerando as particularidades e características de cada espécie de tratamento.

A realidade da *IoT* representa uma ruptura da estrutura de mundo tal qual o conhecíamos e introduz tecnologias, operações e, consequentemente, desafios inexistentes no tratamento de dados seja por meios analógicos, seja por meios digitais "tradicionais". Assim, parece recomendável uma análise dos conceitos introduzidos no RGPD sob a perspectiva dos avanços tecnológicos da Internet das Coisas para permitir uma interpretação da lei condizente com essa nova realidade.

O artigo 4.º do RGPD elenca diversos conceitos, definindo-os com o objetivo de emprestar a esses termos a precisão necessária à interpretação da lei. De partida, cabe-nos à análise do próprio conceito de "dados pessoais", pois a qualificação como "pessoal" dos diversos dados coletados pelos dispositivos de *IoT* é o que definirá a aplicabilidade ou não da proteção do Regulamento.

A norma, neste aspecto, estabelece ser dado pessoal toda "*informação relativa a uma pessoa singular identificada ou identificável (...)*". Note-se que, partindo-se desse conceito, nem todos os dados coletados pelos sensores da Internet das Coisas ou compartilhado entre os diversos aparelhos interconectados estão abrangidos pelo conceito de "dados pessoais"; por exemplo, quando estivermos diante de dados ambientais como a temperatura de uma dada localidade ou o índice de umidade do ar. Isoladamente, os dados ambientais não se referem a nenhuma pessoa e, portanto, podem ser coletados e tratados sem as amarras do RGPD. Porém, associados a outros dados coletados, esses sim qualificados como pessoais, certos dados "não pessoais" podem integrar um feixe de informações, consideradas como "pessoais" em seu conjunto.

O GT29, na Opinião 4/2007[122], estabeleceu, ainda na vigência da Diretiva 95/46/CE, as balizas para interpretação do conceito de "dados pessoais". Embora a redação do RGPD não coincida integralmente com o texto da Diretiva revogada, o núcleo da definição legal permaneceu inalterado, pois concentrado nos termos *qualquer informação*, *relativa*, *pessoa singular*, *identificada ou identificável*.

Ao usar o termo *qualquer informação*, o Regulamento demonstra seu claro objetivo de fincar definição de abrangência ampla. Disso se extrai que são consideradas "dados pessoais" informações de qualquer natureza, seja objetiva ou subjetiva, como as opiniões e os sentimentos. Também, para configurar "dado pessoal" não é necessário que a informação seja verídica ou esteja provada, tanto que o próprio RGPD garante ao titular o direito de solicitar retificação, atualização ou apagamento de dados incorretos ou falsos. A amplitude do termo também permite concluir que os dados pessoais podem apresentar formatos e ter conteúdos dos mais diversos e vão desde informações estritamente sigilosas e sensíveis, como histórico médico, passando por conversas e informações relativas ao seio doméstico e familiar, até comportamentos em ambientes de trabalho e social[123].

O termo *relativa*, embora de significado evidente, permite igualmente algumas colocações relevantes. Certamente, qualquer informação sobre alguém, é facilmente classificada como "dado pessoal", inexistindo, portanto, dificuldades em reconhecer a pessoalidade de informações como nome, data de nascimento, tipo sanguíneo, perfil em uma rede social ou histórico de navegação em dispositivo pessoal. Porém, conforme destaca o GT29, algumas informações podem constituir dados pessoais, mesmo que, de modo imediato, se refiram a coisas[124]. No caso dos dispositivos de *IoT*, pode-se imaginar o exemplo relativo aos frigoríficos inteligentes que mantêm uma lista de compras com alimentos em falta ou de produtos próximos de atingir o prazo de validade. Esses dados podem ser tratados unicamente com o fim de avaliar a periodicidade de reposição de dado produto, ou sua durabilidade

---

122 GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Opinion 4/2007 on the Concept of Personal Data*. Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (Consulta em 01.07.2021)

123 Interessantes exemplos são trazidos pelo GT29 a demonstrar a diversidade dos dados pessoais: a gravação da voz de alguém em uma chamada de *telemarketing*, as imagens de alguém capturadas por câmeras de vigilância (desde que seja reconhecível a pessoa) e, ainda, o desenho de um criança colhido em um teste psiquiátrico realizado no contexto de uma lide judicial. GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Op. Cit.,* p. 8.

124 Os exemplos colacionados na Opinião 4/2007 se referem ao valor de um certo imóvel e ao histórico de manutenção de um carro. Em ambos os casos, os dados tanto podem ser analisados de modo impessoal (e. g. aferição do valor do metro quadrado em determinada zona), quanto pessoal (e. g. avaliar o tamanho do patrimônio do proprietário para fins fiscais, no caso do imóvel, ou mensurar a produtividade do mecânico, no caso do veículo). GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Op. Cit.* pp. 9/10.

média, mas se associados ao perfil do residente podem configurar dados de comportamento.

Para sistematizar a qualificação de uma informação como relativa ou não a uma pessoa, o GT29 afirma que, além do conteúdo dos dados, objetivamente considerado, deve-se analisar também as circunstâncias do tratamento desses dados, pois o caráter pessoal pode decorrer igualmente da finalidade do tratamento ou, ainda, do seu resultado prático. Exemplo disso são os mecanismos de rastreamento de veículos utilizados pelas empresas gestoras de táxis, no exemplo citado na Opinião 4/2007[125], ou atualmente pelas plataformas eletrônicas de transporte tipo TVDE[126]. O sistema de localização se refere, numa perspectiva imediata, ao veículo e não ao motorista (conteúdo) e a finalidade não é a de rastrear a pessoa, mas de possibilitar a ligação entre o passageiro e o carro mais próximo, bem como de fornecer uma estimativa de tempo ao cliente. Contudo, esses mesmos dados podem basear certas conclusões acerca do comportamento dos motoristas, como excesso de velocidade ou condução imprudente, tendo como resultado sua penalização.

Sob a perspectiva da Internet das Coisas, mostra-se relevante ponderar a facilidade com a qual uma informação de conteúdo objetivamente impessoal pode ser associada a outros elementos de modo a impactar na esfera pessoal de alguém. Tal circunstância decorre da ubiquidade dessa tecnologia, notadamente potencializada por sensores, gravadores e câmeras associadas aos dispositivos, somada ao volume de dados coletados (*Big Data*), compartilhados entre dispositivos e cruzados com o objetivo de extrair as mais diversas conclusões a respeito das pessoas.

A análise da pessoalidade do dado sob a perspectiva do resultado, nas hipóteses em que conteúdo e finalidade sejam impessoais, também se apresenta especialmente relevante em um meio tecnológico baseado em *machine learning*, à medida em que os resultados obtidos pelas máquinas nem sempre podem ser antecipados ou controlados em sua totalidade. Ou seja, até mesmo dados a princípio impessoais podem influir nos processos de decisão realizados exclusivamente por algoritmos e causarem impacto na vida de uma pessoa[127].

Quanto ao termo *pessoa singular*, não parece merecer grandes digressões. Isso porque, como visto, o direito à proteção de dados no contexto

---

125 GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Op. Cit*. p. 11.

126 Transporte em veículos descaracterizados a partir de plataforma electrónica, modalidade de transporte passageiros regulamentada em Portugal pela Lei n.º 45/2018 de 10 de agosto.

127 Para Bioni trata-se de uma leitura consequencialista da lei, que parte da distinção não entre dados pessoais e dado não pessoais, objetivamente considerados, mas da análise da relação de causa e efeito gerada pela atividade de tratamento na vida de determinado titular. O autor defende, outrossim, que tal leitura da norma só se justifica a partir da proteção dos direitos da personalidade. Bruno Ricardo Bioni, *Proteção de Dados Pessoais: a função e os limites do consentimento.* Rio de Janeiro, Forense, 2019, p. 78/81.

europeu derivou da proteção dos direitos de personalidade e, portanto, são titulares os seres humanos vivos e não, por exemplo, uma pessoa coletiva.

Por fim, cabe a análise da relevância da expressão *identificada ou identificável*. É certo que a forma mais simples de identificar um dado pessoal parte da correlação dessa informação com o nome da pessoa. Mas, como é óbvio, essa não é a única maneira de identificar o titular de determinado dado. Sobretudo nas modalidades de tratamento em que são elaborados perfis, para análise estatística ou tomada de decisões, o titular de uma informação pode ser identificado mesmo sem menção ao seu nome e quanto mais preciso for o perfil e maior o volume de dados, mais fácil será essa identificação.

Nesse tocante, o considerando 26 do RGPD estabelece que para aferir se o titular de determinado dado é identificável deve-se considerar "*todos os meios suscetíveis de ser razoavelmente utilizados*". Por isso, é possível concluir que na era do *machine learning* e do tratamento de dados por algoritmos, o espectro do que se considera *identificável* é ampliado. Isso porque, buscas, análises e cruzamentos de dados considerados impossíveis ou absurdamente custosos à ação humana podem ser rapidamente operados pelas máquinas. Soma-se, então, de um lado a velocidade operacional dos computadores e dispositivos e, de outro, a imensa capacidade de armazenamento de dados e o resultado é a potencialização da capacidade de identificação de uma pessoa a partir de um registro aparentemente impessoal ou anonimizado.

No caso dos dispositivos *IoT*, é importante mencionar duas características que também permitem uma maior facilidade na identificação do titular de um dado coletado.

Primeiro, pela sua pretensão de personalizar a experiência do usuário, boa parte desses dispositivos são de utilização individual (como é o caso dos relógios *smartwatch* e da maioria dos dispositivos tipo *wearable*, além de outros já utilizados na área da saúde como *intimate contact sensors*, *ingestible sensors* e *implantable sensors*[128]) ou restrita a um ambiente com um número limitado de pessoas, como o ambiente doméstico (caso dos assistentes eletrônicos, cuja utilização é restrita, regra geral, aos moradores de uma casa ou aos ocupantes de um escritório). Portanto, qualquer informação coletada, seja por seus próprios sensores, seja pela transferência de dados a partir de outro dispositivo a ele conectado, é facilmente associada ao seu dono ou relacionada a um dos poucos usuários.

Segundo, a coleta desses dados é realizada comumente por meio de câmeras e sensores biométricos, através do tratamento de dados personalíssimos como impressões digitais, voz e reconhecimento facial. Logo, quanto mais dispositivos interconectados e mais eficientes os sensores, mais precisa é a identificação do titular de cada informação.

---

128 Scott R. Peppet, "Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent.", *in Texas Law Review*, 2014, p. 98.

Outro conceito elencado no artigo 4.º do RGPD com especial relevância para o campo da Internet das Coisas é o de "definição de perfis". O GT29 já direcionou seus estudos à análise das definições de perfis como suporte das decisões automatizadas, elaborando uma série de orientações[129]. Já de início, o documento destaca os aspetos positivos e negativos desse tipo de funcionalidade, que, ao mesmo tempo, garante aumento de eficiência e economia de recursos, trazendo ganhos nos campos da saúde, educação, transportes, mas também representando um risco significativo para os direitos e as liberdades das pessoas[130]. A norma estabelece que "definição de perfis" constitui qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados para avaliar certos aspetos pessoais de uma pessoa singular, tais como situação económica, saúde, preferências e comportamentos de uma maneira geral[131].

Ou seja, a definição de perfis envolve desde a recolha de dados pessoais para essas finalidades, passando por uma análise automatizada para identificar correlações (total ou parcialmente sem intervenção humana), até resultar na aplicação dessas conclusões a uma pessoa, identificando padrões comportamentais e classificando o indivíduo de acordo, por exemplo, com sua capacidade para executar uma tarefa, seus interesses ou comportamentos futuros presumíveis[132].

Note-se que o conceito legal estabelece que o tratamento é automatizado, porém a tomada de decisão (terceira fase do processo) pode ou o não o ser. Ou seja, a definição de perfis nem sempre está atrelada a decisões automatizadas. Ao analisar um pedido de empréstimo, a instituição financeira muitas vezes recorre à avaliação do perfil do solicitante, que pode ter a forma, por exemplo, de um sistema de *score* proporcional ao risco de inadimplemento baseado em uma série de dados comportamentais. A decisão acerca da concessão ou não do empréstimo pode ser realizada tanto por um ser humano (definição de perfil sem decisão automatizada), quanto por uma máquina através de algoritmo e com base em dados coletados por diversos outros dispositivos a ela conectados (definição de perfil usada para basear uma decisão automatizada). Igualmente, pode haver decisão automatizada sem definição de perfil, notadamente na hipótese de dispositivos acoplados a sensores, como nos casos das coimas de trânsito aplicadas automatica-

129 GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*. Outubro, 2017. Rev. Fevereiro, 2018. Disponível em file:///C:/Users/User/Downloads/guideline%20decis%C3%B5es%20automatizadas%20e%20profilling.pdf (Consulta em 05.08.2021).

130 GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Op. Cit.* p. 5.

131 Madalena Perestrelo de Oliveira, *Op. Cit.,* p. 63.

132 Grupo De Trabalho Do Artigo 29.º Para A Proteção De Dados. *Op. Cit.* p. 7/8.

mente quando um radar deteta o excesso de velocidade de um veículo ou uma câmera o avanço ao sinal vermelho[133].

Como já mencionado, um dos atributos dos objetos inteligentes é a personalização da experiência, pois à medida em que o usuário utiliza o dispositivo e este acumula dados acerca do seu comportamento, funcionamento do seu corpo e particularidades individuais, a máquina, através de seus algoritmos, adquire a capacidade de antecipar a vontade do usuário, tomando decisões por ele. Ou seja, a partir dos dados coletados, o dispositivo elabora conclusões acerca da personalidade do indivíduo, o que gera especial preocupação com a possibilidade de decisões automatizadas discriminatórias[134] ou de tratamento de dados de forma a expor a reputação do titular ou causar-lhe prejuízo financeiro, como destacado no considerando 75 do RGPD. O mesmo considerando também resaalta a preocupação com a definição de perfis relativos a pessoas vulneráveis. Nesse ponto, mister mencionar a problemática acerca da incapacidade de a máquina distinguir um vulnerável de um não vulnerável ou mesmo dados comuns dos dados sensíveis.

Tudo isso justifica um tratamento específico pelo RGPD em relação à definição dos perfis e decisões automatizadas, conforme disciplinam os artigos 21.º e 22.º. Por sua vez, o considerando 71 impõe limitações à prática, ressaltando o direito do titular de não ficar sujeito a ela e também o resguardo das crianças em relação a esse tipo de tratamento. Contudo, no caso da Internet das Coisas os dispositivos devem ser interpretados com a cautela devida, pois sua interpretação restritiva pode inviabilizar a própria tecnologia base dos dispositivos. A seguir, detalharemos a regulamentação específica do RGPD acerca das definições de perfis e decisões automatizadas e os desafios dela decorrentes em relação à Internet das Coisas.

O artigo 4.º também traz o conceito de "responsável pelo tratamento" como sendo a pessoa singular ou coletiva que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais. No âmbito da Internet das Coisas, identificar esse(s) responsável(eis) pode se apresentar como tarefa especialmente difícil. Isso porque, uma fabricante de frigorífico, por exemplo, que lança ao mercado um produto *smart*, provavelmente, não será a responsável direta pelo desenvolvimento da inteligência artificial a ele associada, componente comumente contratado de uma empresa de tecnologia. Ademais, esse dispositivo pode ser conectado, pelos usuários, a outros dispositivos, desenvolvidos por outras empresas, formando uma rede de compartilhamento dados. Note-se, por isso, que não raras são as hipóteses em que nenhuma das empresas está integralmente no controlo das finalidades e dos meios de tratamento, pois a operação se dá sem qualquer intervenção humana.

---

133 Grupo De Trabalho Do Artigo 29.º Para A Proteção De Dados. *Op. Cit*. p. 8.

134 Madalena Perestrelo de Oliveira*, Op. Cit*., p. 63.

Nesse tocante, o artigo 26.º do RGPD introduz as figuras dos "responsáveis conjuntos", para as hipóteses em que dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento. Ao passo que os artigos 27.º e 28.º estabelecem regras específicas para essa hipótese, definindo as responsabilidades de cada um desses corresponsáveis. A questão posta em relação aos dispositivos de *IoT* diz respeito a essa posição de controlo em relação à atividade de tratamento, que na prática é integralmente realizada pelo dispositivo. Além disso, quanto às configurações e aos limites do tratamento, muitas vezes, são definições que cabem não às empresas desenvolvedoras, mas ao próprio usuário do dispositivo, sendo ele não raro quem decide inclusive acerca do tratamento de dados de terceiros coletados pelo seu dispositivo. Assim, já há teses defensoras da possibilidade de inclusão do proprietário do dispositivo entre o rol de "responsáveis pelo tratamento"[135], em aplicação análoga às decisões do TJUE nos casos *Wirtschaftsakademie*[136] e *Jehovah's Witness*[137], ambos os julgamentos ainda sob a vigência da Diretiva Diretiva 95/46/CE.

Por fim, cabe uma análise específica do conceito de "consentimento" trazido pelo Regulamento e suas implicações no âmbito da *IoT*, pois, embora o consentimento não seja a única base legal para legitimar o tratamento de dados, é uníssono que ele compõe núcleo central da norma, tamanha a sua evidência.

O RGPD, no artigo 4.º, n.º 11, assim define consentimento: *manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.*

Quanto à manifestação de vontade, essa é constituída por dois elementos: primeiro, a vontade humana e, depois, sua exteriorização[138]. Note-se que essa exteriorização não pressupõe obrigatoriamente uma declaração, seja oral ou escrita. Há diversas formas de exteriorizar uma vontade, exigindo a lei apenas que, se não declarada, seja resultado de um ato positivo inequívoco. No caso de um dispositivo de Internet das Coisas a simples aquisição do equipamento pode ser interpretada como uma manifestação de vontade. Ora, se alguém resolve comprar determinado dispositivo, mani-

---

135 Acerca do tema: Silvia De Conca. "Between a Rock and a Hard Place: Owners of smart speakers and joint control", *in SCRIPTed*, n.º 2, Vol. 17, 2020. pp. 238-268.

136 Em que o TJUE entendeu que configuram responsáveis conjuntos o *Facebook* e o administrador de uma página de fãs criada na rede social. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62016CJ0210&from=PT [Consulta em Agosto de 2021]

137 Em que o TJUE entendeu que configuram responsáveis conjuntos a comunidade religiosa e cada um de seus membros em relação ao tratamento de dados realizados no contexto da pregação porta a porta. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62017CJ0025&from=PT (Consulta em 01.08.2021)

138 António Barreto Menezes Cordeiro, "O consentimento do titular dos dados no RGPD", *in FinTech: desafios da tecnologia financeira.* coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte. Vol. 2. Almedina, Coimbra, 2017.

festa com aquele ato a vontade de utilizá-lo, assumindo as consequências naturais decorrentes daquele uso.

Quanto ao caráter da liberdade, a princípio toda vontade manifestada, por exemplo, por meio da compra de um dispositivo é livre, mas em casos excepcionais essa liberdade pode ser questionada, como nas hipóteses de coação, de uma compra imposta como condição para outro negócio jurídico, como uma exigência do empregador no curso de uma relação de trabalho ou eivada de quaisquer dos vícios de vontade elencadas no Direito Civil[139]. Em resumo, não poderá ser considerada de livre vontade a manifestação se ela não decorrer de uma escolha verdadeira ou, ainda, quando não puder recusada ou revogada sem que o titular dos dados seja prejudicado, conforme estabelece o considerando 42, *in fini*.

Ademais essa manifestação deve ser específica. Logo, será inválido o consentimento dado de forma genérica, sob pena de se transformar o consentimento em uma autorização ilimitada para o responsável pelo tratamento tratar todo e qualquer dado de determinado titular. Dessa especificidade necessária, surge a exigência da granularidade. O consentimento deve ser granular à medida em que, sendo mais de uma as finalidades de tratamento, deve ser garantido ao titular consentir com cada uma isoladamente[140].

A ausência de granularidade no consentimento representa um dos grandes desafios para o tratamento dos dados por dispositivos de *IoT*, pois na hipótese de o tratamento basear-se no consentimento, caso o titular não esteja de acordo com todas as finalidades de tratamento, a única opção que lhe resta é a não aquisição do dispositivo ou sua não utilização, pois não pode ele opor-se a uma ou mais finalidades de tratamento. Assim, não raras são as críticas ao protagonismo pelo RGPD ao consentimento como meio de legitimação do tratamento de dados apesar da evidente falta de opção do titular, que na maioria das vezes tem que exercer sua escolha com base no "tudo-ou-nada": permitir o tratamento dos seus dados beneficiando-se do mundo digital ou ficar alheio ao desenvolvimento tecnológico para proteger-se da vigilância exercidas pelas corporações detentoras de dados[141].

Ainda, essa manifestação de vontade deve ser informada. A exigência aparece como corolário do princípio da transparência e intimamente ligado ao objetivo do RGPD de garantir efetivo controlo dos seus dados pelos titulares. Até porque, sequer é possível falar propriamente em vontade livre

---

139 Em defesa da aplicação do Direito Comum na seara da proteção de dados quando com ela não seja incompatível: António Barreto Menezes Cordeiro, *Op. Cit.,* p. 42.

140 Grupo De Trabalho Do Artigo 29.º Para A Proteção De Dados. *Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679.* Novembro, 2017, disponível em file:///C:/Users/User/Downloads/20180416_article_29_wp_guidelines_on_consent_publish_09A6854F-F638-8898-7A0543CE0857250F_51030.pdf (Consulta em 02.08.2021), p. 11.

141 Marcin Betkier. Privacy Online, Law and the Effective Regulation of Online Services. Cambridge, Intersentia, 2019.

e manifestação específica sem atrelar esses elementos ao conhecimento do titular em relação as circunstâncias relevantes para sua decisão. Entre as informações mínimas que devem ser prestadas, para o GT29[142], estão: i) identidade do responsável pelo tratamento; ii) finalidade de cada uma das operações de tratamento; iii) quais dados são recolhidos; iv) o direito do titular de retirar o consentimento; v) informações acerca da utilização dos dados para decisões automatizadas em conformidade com o artigo 22.º, n.º 2, *c)*; vi) possíveis riscos de transferências de dados (artigo 46.º).

No caso da Internet das Coisas, essa informação também se apresenta como um importante desafio. Primeiro, porque o caráter da novidade intrínseco a esses avanços tecnológicos vem acompanhado de um desconhecimento acerca de todas consequências e impactos dessa tecnologia na vida das pessoas. No caso da *IoT* há, inclusive, muito desconhecimento de seus limites pela própria comunidade científica e, por consequência, desconfiança dos usuários. Segundo, porque boa parte dos dispositivos não dispõe de ecrã ou possui um de pequenas dimensões de modo que não são compatíveis com o objetivo de comunicar ao seu utilizador um grande número de informações, de maneira clara e em linguagem acessível[143]. Essas dificuldades já foram evidenciadas pelo GT29, no Parecer 8/2014, quando a entidade ponderou que os mecanismos clássicos utilizados para obter o consentimento dos indivíduos comumente não se mostram compatíveis com os dispositivos inteligentes, o que pode resultar num consentimento de baixa qualidade[144].

Por fim, o RGPD exige que a manifestação de vontade seja explícita. Importante mencionar que o vocábulo *"explícita"*, apesar de constar da Proposta de RGPD apresentada inicialmente pela Comissão Europeia[145], foi suprimido da versão final do texto normativo nas demais versões, mas não na portuguesa[146]. A supressão foi resultado da consagração da posição defendida pelo Conselho da União Europeia para evitar a interpretação segundo à qual o consentimento haveria de ser escrito.

---

142 Grupo De Trabalho Do Artigo 29.º Para A Proteção De Dados. *Op. Cit.,* pp. 14/15.

143 Grupo De Trabalho Do Artigo 29.º Para A Proteção De Dados. *Orientações relativas à transparência na aceção do Regulamento 2016/679*. Novembro, 2017, disponível em https://www.uc.pt/protecao-de-dados/suporte/20180411_orientacoes_relativas_a_transparencia_wp260_rev01 (Consulta em 02.08.2021)

144 Grupo De Trabalho Do Artigo 29.º Para A Proteção De Dados. *Opinion 8/2014 on the on Recent Developments on the Internet of Things.* Setembro, 2014. Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (Consulta em 13.07.2021)

145 Comissão Europeia. Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52012PC0011&from=sl (Consulta em03.08.2021)

146 António Barreto Menezes Cordeiro, O consentimento do titular dos dados no RGPD. Op. Cit., p. 40.

Embora a versão em português não tenha acompanhado as demais, certamente o conhecimento do desfecho das negociações quando da aprovação do texto direcionam a interpretação do termo "explícita", que deve ser encarado como antônimo de "implícita" no sentido de que o consentimento não pode ser presumido ou resultar de atos negativos, como o silêncio ou a inércia.

5. A (APARENTE) INCOMPATIBILIDADE ENTRE O RGPD E O TRATAMENTO DE DADOS REALIZADO PELOS DISPOSITIVOS DE *IOT*

Enquanto a implementação da Internet das Coisas com suas caraterísticas de ubiquidade, hiperconectividade e omnipresença inaugurou uma nova era tecnológica marcada por um volume inédito de dados tratados, o Regulamento Europeu de Proteção de Dados surge como resultado da evolução histórica da legislação de proteção de dados pessoais, assentado, portanto, em conceitos e premissas que remontam a períodos em que o progresso tecnológico alcançava níveis consideravelmente inferiores de automação.

É esse o cenário que serve de pano de fundo para o debate acerca de uma aparente incompatibilidade entre o RGPD e a realidade da *Internet of things* e que permite as não raras críticas aos Regulamento no sentido de ele já ter nascido obsoleto ou de representar entrave inconveniente ao desenvolvimento tecnológico.

Acerca do assunto, Zarsky[147] publicou já em 2017, antes, portanto, da entrada em vigor do Regulamento mas depois da sua aprovação, um estudo crítico do RGPD apontando incompatibilidades na norma em relação aos atuais avanços tecnológicos. Embora não tenha tratado especificamente da *IoT*, Zarsky elencou quatro aparentes conflitos entre RGPD e a "Era do *Big Data*": o princípio da limitação das finalidades (artigo 5.º, 1, *b)*), o princípio da minimização dos dados (artigo 5.º, 1, *c)*), as categorias especiais de dados (artigo 9.º) e a regulação específica das decisões automatizadas (artigo 22.º).

Também outros questionamentos surgem a partir das restrições legais às decisões automatizadas e os entraves que elas podem implicar no desenvolvimento da inteligência artificial e no funcionamento dos algoritmos. Analisaremos esses questionamentos sob duas perspectivas: o conflito entre o princípio da transparência e a opacidade da inteligência artificial (efeito *black-box*); e a incompatibilidade entre o *machine learning* e o direito ao esquecimento.

---

147 Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data*"*, *in Seton Hall Law Review*, n.º 4, Vol. 47, 2017. pp. 995-1020. Disponível em https://heinonline.org/HOL/P?h=hein.journals/shlr47&i=1019 (Consulta em 30.7.2021)

5.1. O IMPACTO DO PRINCÍPIO DA LIMITAÇÃO DAS FINALIDADES (ARTIGO 5.º, N.º 1, *B)* DO RGPD)) NO TRATAMENTO DE DADOS PELOS DISPOSITIVOS DE IOT

Conforme já introduzimos no item 3.1, o princípio da finalidade estabelecido no artigo 5.º, n.º 1, *b)*, do RGPD exige que os dados sejam recolhidos para finalidades, além de legítimas, determinadas e explícitas. Além disso, há uma vedação ao tratamento posterior para finalidades incompatíveis com as primeiras (aquelas que justificaram a recolha). Nesse quesito, a própria norma cuida de elencar três exceções muito específicas: interesse público, investigação científica ou histórica e fins estatísticos.

Ou seja, o Regulamento parte da premissa de que a finalidade precede à coleta dos dados, sendo esta última uma ação necessária à consecução daqueles fins primeiros.

Por outro lado, a realidade do Big Data – e, por consequência, da Internet das Coisas – parte de premissa inversa, segundo a qual o devem ser recolhidos os dados para, posteriormente, tratá-los para finalidades cuja possibilidade sequer era antecipada. Isso porque o ponto central do desenvolvimento da inteligência artificial é o de superar os limites da inteligência humana, não só por meio da obtenção de uma maior velocidade de processamento de informações e capacidade de armazenamento, mas realizando atividade tidas por impossíveis ou inimagináveis em uma realidade sem máquinas inteligentes.

Nesse cenário, é mister ressaltar que embora a inteligência artificial seja programada, em alguns aspectos, para espelhar o modo de pensar humano e potencializar seus resultados, em outros aspectos, a máquina supera os limites da mente humana rompendo com o padrão por ela seguido e adotando um novo padrão, invisível aos nossos olhos, dada a nossa limitada capacidade de armazenamento de informações. Para descobrir esses novos padrões, é indispensável a coleta massiva de dados para uma finalidade que só vai ser evidenciada a *posteriori*.

Por isso, Zarsky[148] destaca que, o cumprimento do RGPD no tocante à limitação das finalidades, as entidades engajadas em qualquer atividade que envolva análise de *Big Data* estariam obrigadas a monitorar de modo ininterrupto suas operações de modo a fiscalizar se estariam sendo excedidas as finalidades antecipadas ao titular quando da recolha dos dados, exigência impossível de ser cumprida ou, ao menos, extremamente difícil e custosa. Em alternativa, caberia a essas entidades tentar driblar o entrave legal, informando os titulares das finalidades abrangentes, correndo, todavia, o risco de ter sua finalidade considerada inespecífica e, portanto, ilegítima sob a perspectiva do Regulamento.

Para além desse obstáculo que o princípio da limitação das finalidades impõe à Internet das Coisas, impondo restrições diretas aos seus meios de funcionamento, há também os entraves indiretos. Por exemplo, as restri-

148 Tal Z. Zarsky, *Op. Cit.,* p. 1006.

ções decorrentes do princípio acabam por dificultar o acesso de pequenas empresas e *startups* ao mercado de dados e concentram o poder nas mãos das chamadas "gigantes da tecnologia" (*Big Techs*). Por isso, para Zarsky, o princípio também é conflitante com a era do *Big Data* na medida em que diminui o ambiente de competição necessário à inovação[149].

Contudo, a realidade é que a limitação da finalidade não é apenas mais uma regra – a qual poderia ter sua aplicação flexibilizada a depender do tipo de tecnologia utilizado no tratamento de dados pessoais[150]– mas representa uma das pedras angulares do Regulamento. Então, eventual conclusão no sentido de ser impossível a compatibilização entre o princípio e o *Big Data* e, por consequência, a Internet das Coisas, resultaria na defesa da inaplicabilidade de todo o diploma a essa seara.

Zarsky[151], nesse tocante, apresenta algumas soluções. A primeira, de ordem prática, sugere um monitoramento rigoroso do uso dos dados com o fim de promover a confiança e conter abusos por partes dos responsáveis pelo tratamento. Assim, o controlo pretendido pelo Regulamento seria efetivado não por meio de uma proibição impeditiva ao tratamento (*ex ante*), mas por meio de limitação posterior sempre que o uso dos dados se revele abusivo[152].

A segunda solução se relaciona com o seguinte trecho do dispositivo regulamentar: "não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades". Segundo o autor, a compatibilização com o RGPD perpassa pela interpretação do termo "incompatível", ao passo que o tratamento de dados posterior, para finalidades diversas da inicialmente informada ao titular, seria admissível desde que não fossem incompatíveis entre si. Ou seja, o vocábulo incompatível não pode ser interpretado de forma restritiva de modo a concluirmos que as finalidades de tratamento devam ser as exatas finalidades pretendidas quando da recolha dos dados; elas podem ser diferentes, desde que não incompatíveis.

Nesse quesito, é importante analisar o teor do artigo 6.º, n.º 4, do RGPD que determina que o responsável pelo tratamento, para fins de verificação da compatibilidade entre as finalidades, primeira e posterior, deve ter em conta: a) qualquer ligação entre a finalidade para a qual os dados pessoais

---

149 Tal Z. Zarsky, *Op. Cit.,* p. 1007.

150 Até porque isso violaria a neutralidade expressa no considerando 15. Sobre o assunto: Ugo Pagallo. "The legal challenges of Big Data: putting secondary rules first in the field of EU Data Protection"*, in European Data Protection Law Review (EDPL)*, n.º. 1, Vol. 3, 2017, pp.36-46.

151 Tal Z. Zarsky, *Op. Cit.,* p. 1007.

152 Tal Z. Zarsky, "Desperately Seeking Solutions: Using implementation-based solutions for the troubles of information privacy in the age of data mining and the internet society.", *in Maine Law Review*, n.º 1. Vol. 56, 2004, pp. 13-60, disponível em: https://heinonline.org/HOL/Page?public=true&handle=hein.journals/maine56&div=7&start_page=13&collection=journals&set_as_cursor=0&men_tab=srchresults (Consulta em 16.08.2021)

foram recolhidos e a finalidade do tratamento posterior; b) o contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento; c) a natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.º, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.º; d) as eventuais consequências do tratamento posterior pretendido para os titulares dos dados; e e) a existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

Apesar das dificuldades práticas de aplicação desses parâmetros na seara do *Big Data* e da inteligência artificial, certo é que a compatibilização entre o princípio da limitação das finalidades e o funcionamento da IoT perpassa obrigatoriamente por uma interpretação do texto normativo que flexibilize a rigidez das suas restrições.

5.2. O PARADOXO ENTRE O PRINCÍPIO DA MINIMIZAÇÃO DOS DADOS E O VOLUME DE DADOS ENVOLVIDOS NAS ANÁLISES *BIG DATA*

O princípio da minimização dos dados (artigo 5.º, n.º1, *c)* do RGPD) constitui outra pedra angular do Direito da Proteção dos Dados, mas, diferentemente do princípio da limitação das finalidades[153], não tem origem *constitucional*. Para Zarsky, essa particularidade permite uma maior margem de flexibilização ao legislador europeu quanto à abrangência do princípio [154].

Do princípio da minimização é possível deduzir restrições ao tratamento de dados em várias perspectivas como, por exemplo, no momento da recolha, com a limitação do escopo e categoria dos dados coletados, mas também em relação ao período de tempo que os dados permanecem armazenados[155]. A lógica por trás do princípio é simples: quanto menos dados à disposição do responsável pelo tratamento – seja porque já deletados, seja porque sequer coletados – menores as chances de haver utilização abusiva de dados, para além do consentimento do titular, por exemplo, e também menores os riscos de segurança ou menor o impacto de eventual vazamento.

Na contramão dessa lógica, a realidade do *Big Data* parte da premissa segundo a qual quanto maior for o volume de dados recolhido e armazenado, mais precisas serão as análises possíveis, mais útil será o tratamento

---

153 Extraído da expressão "*para fins específicos*" constante do Artigo 8.º, n. 2, da Carta dos Direitos Fundamentais da União Europeia.

154 Tal Z. Zarsky, *Op. Cit.,* p. 1009.

155 Daí decorre a obrigação do responsável pelo tratamento de estabelecer prazos para apagamento dos dados pessoais, conforme texto do considerando 39: "(...) A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica. (...)"

desses dados e melhor decisões poderão ser tomadas pelas máquinas sem a intervenção humana.

Ou seja, salta aos olhos o paradoxo emergente da aplicação de uma legislação que determina a restrição da coleta e armazenamento de dados "ao mínimo necessário" a tecnologias baseadas em análises por meio de algoritmos e máquinas inteligentes, cujo funcionamento pressupõe um volume considerável de dados, para deles extrair padrões de comportamento e daí conseguir prever escolhas do usuário e se amoldar às suas preferências. Ademais, a exclusão dos dados ou a coleta restritiva causa lacunas capazes de impedir o bom funcionamento dos algoritmos, provocando distorções, diminuindo a qualidade sua performance e, consequentemente, sua utilidade[156].

Nesse tocante, Zarsky sugere que uma solução para essa incongruência entre a análise de *Big Data* e o RGPD emerge da exceção legal em relação ao tratamento de dados para fins estatísticos (artigo 5.º, n.º 1, *b), in fine*), bem como a pseudonomização (artigo 6.º, n.º 4, *e)*), sem deixar de ressaltar, entretanto, que nem sempre essa estratégia será possível e, em alguns casos, a pseudonomização pode restringir consideravelmente os benefícios decorrentes do tratamento[157].

Já Peter K. Yu, defende o compartilhamento de dados entre os controladores, notadamente as grandes plataformas e os controladores de dispositivos inteligentes por meio de uma maior *interoperatividade* entre as bases de dados e esforços no sentido de garantir a portabilidade dos dados. Para o autor, essa *interoperatividade* não só potencializa a utilidade dos dispositivos para seus usuários, como contribui para uma maior competitividade no setor da inteligência artificial e induz a avanços tecnológicos, inclusive em relação à segurança da informação[158].

5.3. A PROIBIÇÃO AO TRATAMENTO DE CATEGORIAS ESPECIAIS DE DADOS (DADOS SENSÍVEIS) E A IMPOSSIBILIDADE PRÁTICA DE MÁQUINAS INTELIGENTES DISTINGUIREM A NATUREZA DOS DADOS

O artigo 9.º do RGPD, assim como já fazia a Diretiva 95/46/CE, cria categorias especiais de dados pessoais a partir da sua potencialidade em revelar informações sensíveis acerca do indivíduo, notadamente as que podem lhe expor a tratamento discriminatório ou as que dizem respeito às esferas mais íntimas. Por isso, a norma proíbe, em linhas gerais, o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical e, ainda, dados genéticos, biométricos ou os relativos à saúde, à vida e a orientação sexual.

---

156 Peter K. Yu, "Beyond Transparency and Accountability: Three additional features algorithm designers should build into intelligent platforms.", *in Northeastern University Law Review*, n.º 1, Vol. 13, 2021, pp. 263-296.

157 Tal Z. Zarsky, *Op. Cit.,* p. 1011.

158 Peter K. Yu, *Op. Cit.,* p. 291.

O próprio disposto cuida de estabelecer uma série de situações em que o tratamento de dados dessa natureza será considerado legítimo, por exemplo, na hipótese de ser dado o consentimento explícito pelo titular em relação a finalidades específicas (artigo 9.º, n.º 2, *a)*) ou quando o tratamento disser respeito à proteção de interesses vitais do titular ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento (artigo 9.º, n.º 2, c)).

O maior desafio, no que toca à Internet das Coisas, emerge do fato de não ser possível a princípio o controlo e seleção por dispositivos inteligentes da natureza dos dados em tratamento. A primeira dificuldade surge da própria elasticidade do conceito. Por exemplo, em relação aos dados relativos à saúde, incluído nas categorias especiais, o considerando n.º 35 estabelece que "*deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. (...)"*.

Ou seja, um dado aparentemente sem qualquer relação com a saúde de uma pessoa singular poderá, dentro de certo contexto, revelar informações relacionadas à saúde, fazendo incidir as restrições legais em relação ao seu tratamento. No contexto atual da pandemia de Covid-19, por exemplo, isso pode ser bem observado em relação aos dados que indicam a procedência geográfica de passageiros. A princípio, origem e destino de um viajante ou informações constantes de uma passagem de avião, em nada se relacionam à saúde do titular dos dados. Contudo, no cenário pandêmico, o local de origem de alguém permite inferir sua exposição potencial ao vírus, bem como a alguma cepa variante característica de determinada localidade.

Portanto, todo dado não estritamente relacionado diretamente com as categorias especiais pode potencialmente revelar, a depender do contexto, informações consideradas sensíveis e atrair um conjunto de regras e proibições distintas das regulares. Não se trata, assim, de um apanhado de dados de natureza objetivamente determinados, mas envolve uma acurada avaliação caso a caso acerca da natureza daquelas informações, o que pode se mostrar impossível de ser realizado por um dispositivo inteligente ou, no mínimo, exigiria um grau de sofisticação de inteligência artificial que inviabiliza o desenvolvimento de novos dispositivos[159].

Além disso, Zarsky pondera que se todo dado pode, em teoria, revelar informações sensíveis, então não existiriam razões para manter a distinção. A manutenção dessas categorias especiais, nesse sentido, teria tão somente um condão simbólico de destacar uma especial atenção à informações potencialmente causadora de tratamento discriminatório. Contudo, prossegue o autor, a sustentar que na era do *Big Data* o tratamento discriminatório mais comum decorre não de conduta intencional a partir de certa informação sensível, mas principalmente é gerado sem intenção, em consequência do mal

[159] Tal Z. Zarsky, *Op. Cit.,* p. 1013.

funcionamento de algoritmo[160]. Ou seja, nesse tocante, a divisão dos dados em categorias geral e especial não atingiria a finalidade almejada à medida em que não teria impacto na ocorrência de tratamento discriminatórios.

Por fim, cita-se outras consequências negativas advindas da criação das categorias especiais: a) a flexibilidade do conceito gera custos regulatórios e judiciais para preencher as lacunas desse conceito aberto; b) essa imprecisão conceitual resulta em insegurança jurídica, provocando desestimulo de investimento e onerando, sobretudo, pequenas empresas com a necessária consultoria jurídica; c) simbolicamente, se todos os dados são qualificáveis potencialmente como pertencentes à categoria especial, na prática, nenhuma informação será considerada especialmente sensível e, ao fim, todos os dados receberão tratamento uniforme e o almejado alto nível de proteção a certos dados será diluído[161].

5.4. AS RESTRIÇÕES LEGAIS ÀS DECISÕES AUTOMATIZADAS E A OPACIDADE DA INTELIGÊNCIA ARTIFICIAL EM CONTRAPONTO AO DEVER DE TRANSPARÊNCIA

O artigo 22.º do RGPD se refere especificamente a normas especiais aplicáveis às decisões automatizadas, sejam ela associadas ou à definição de perfis, conforme tratamos *supra*. A primeira distinção legal imposta para esse tipo de tratamento de dados, que é a base do funcionamento dos dispositivos de *IoT*, é o direito do titular de dados de não ficar sujeito a nenhuma decisão totalmente automatizada (artigo 22.º, n.º 1). Já o artigo 22.º, n.º 2 prevê algumas exceções para a regra geral: a) nas hipóteses necessárias à celebração ou execução de um contrato; b) em hipóteses específicas admitidas pelo Direito Europeu ou de qualquer Estado-Membro, desde que com as necessárias salvaguardas aos direitos e interesses dos titulares; c) por fim, na hipótese de consentimento explícito do titular. Essas exceções, de acordo com o número 4 do mesmo artigo, não se aplicam quando se tratar de dado qualificado nas categorias especiais, o que suscita os desafios descritos acima.

Ainda, o artigo 22.º, n.º 3 estabelece dois direitos aos titulares de dados, nomeadamente o de poder solicitar intervenção humana e o de manifestar oposição à decisão conforme seu ponto de vista.

Zarsky apresenta, em sua visão, os dois principais motivos para o especial tratamento dedicado às decisões automatizadas, sendo o primeiro relacionado com o dever de honra e respeito por partir do pressuposto que o titular, notadamente nas hipóteses de tomadas de decisão que impactam significativamente sua vida, prefere que sua situação seja avaliada por um ser humano. Já o segundo motivo se apresenta como consequência de uma generalizada falta de confiança nas máquinas e sistema tecnológi-

160 Tal Z. Zarsky, *Op. Cit.,* p. 1014.

161 Tal Z. Zarsky, *Op. Cit.,* p. 1015.

cos, razão que vem pouco a pouco perdendo sua força conforme avança o progresso da tecnologia[162].

Portanto, a tensão entre o RGPD e o universo da Internet das Coisas – que envolve naturalmente a inteligência artificial e o *Big Data* – mostra-se das mais evidentes incompatibilidades. Enquanto o Regulamento se preocupa em determinar que o tratamento integralmente automatizado e a submissão dos titulares às decisões daí advindas seja excecional, no mundo *IoT* esse tipo de tratamento é a regra e quanto mais desenvolvida a tecnologia, menor será a necessidade de intervenção humana.

Nesse aspeto, o RGPD atua como freio à inovação e ao progresso tecnológico. Primeiro, por impor entraves ao funcionamento do *Big Data* e minimizar, por consequência, sua eficiência e utilidade; segundo, ainda nos casos excecionais em que é permitido o tratamento pelo RGPD, a operação deve ser realizada de tal maneira que seja "interpretável" ao ser humano, exigindo, muitas vezes, algum tipo de intervenção humana, comprometendo, mais uma vez, a eficiência dos sistemas; terceiro, tudo isso onera consideravelmente a operação e apresenta-se como desestímulo aos investimentos[163].

Outra obrigação imposta pelo Regulamento ao responsável pelo tratamento decorre dos artigos 13.º, n.º 2, *f)* e 14.º, n.º 2, *g)* segundo os quais o titular de dados deve ser informado da existência de decisões automatizadas, bem como acerca da lógica subjacente a elas e as consequências do tratamento. Esse "direito à explicação", na prática, pode se revelar extremamente custoso, quando não impossível, pois não raros são os sistemas em relação aos quais se conhece os dados coletados (*inputs*) e o resultado do tratamento (*outputs*), mas não o procedimento realizado pela máquina para transformar um em outro[164]. Em relação a essa obscuridade da lógica por trás de alguns sistemas inteligentes, os especialistas cunharam o nome de efeito *black-box*.

O termo tem sido utilizado como referência ao caráter da opacidade da Inteligência Artificial, que torna o padrão de procedimento do algoritmo indetectável, em alguns casos, mesmo se submetida à intensa observação humana, pois o acesso ao *output* por si nem sempre permite perceber e reproduzir o sequencial lógico realizado pela máquina, sobretudo porque ele não é constante. A mudança dos padrões utilizados para realizar as operações pemite às máquinas inteligentes um contínuo aprimoramento de sua performance, ao mesmo tempo em que torna sua operação icognoscível. Para Forti, as obrigações impostas pelo Regulamento demonstram que remete a uma época em que os algoritmos da Inteligência Artificial não exerciam importante papel na

162 Tal Z. Zarsky, *Op. Cit.,* p. 1017.
163 Tal Z. Zarsky, *Op. Cit.,* p. 1017.
164 Peter K. Yu, *Op. Cit.,* p. 268.

vida cotidiana e, por isso, resultam numa incompatibilidade entre o funcionamento da IA e o grau de transparência legalmente exigido[165].

A essa problemática acerca da dificuldade de os próprios desenvolvedores e operadores conhecerem as lógicas subjacentes aos procedimentos realizados pelas máquinas inteligentes, soma-se o questionamento acerca da capacidade de os titulares perceberem essa lógica na hipótese desse lhes ser informada. Nesse aspecto, o dever de explicação se mostra pouco útil sob a perspectiva do titular que, mesmo nas situações nas quais é possível compreender a lógica informada, a análise da pertinência e adequação desses procedimentos exige dedicação de tempo, esforços e energia consideráveis[166].

Estabelece-se daí um círculo vicioso: a opacidade dos dispositivos inteligente não permite atingir o grau de transparência esperado pelos usuários, que adquirem e operam os dispositivos sem completo entendimento de como eles funcionam e decidem. Consequentemente, crescem as preocupações com a confiabilidade dessas máquinas e a segurança de seus processos e aumenta a demanda por mais transparência. Esse estado de desconfiança é ainda mais facilmente observado em relação aos dispositivos utilizados na área da saúde (e-*Health*), pois o efeito *black-box* impede médicos e pesquisadores de apreender a lógica dos procedimentos automatizados, trazendo incertezas em relação a soluções e diagnósticos a não ser que confiem no bom funcionamento do algoritmo. Ilustrativo exemplo é trazido por Nahmias e Perel[167] quando mencionam a implementação do mecanismo de *machine learning* no Mount Sinai Hospital, em Nova York. O sistema se provou mais tarde ser extremamente eficiente no tratamento dos dados coletados pelo hospital, sendo capaz de detetar várias doenças, inclusive distúrbios psíquicos como esquizofrenia. Todavia, nem os médicos pesquisadores nem os desenvolvedores alcançar como o algoritmo conseguiu tal feito, tornando impossível a concretização do direito à explicação.

Também em relação à utilização da IA no campo médico, Forti[168] apresenta outros entraves decorrentes dos princípios do RGPD, notadamente o da transparência, tais como a exposição do funcionamento dos dispositivos como desestímulo à inovação por dificultar a proteção da propriedade intelectual e as restrições ao tratamento de certas categorias de dados (além dos estritamente da saúde, os relativos a gênero, raça e outros fatores que influenciam nos diagnósticos, mas podem também resultar em tratamento descriminatórios).

---

165 Mirko Forti, "The Deployment of Artificial Intelligence Tools in the Health Sector: Privacy Concerns and Regulatory Answers within the GDPR.", *in European Journal of Legal Studies*, n.º 1, Vol. 13, 2021, pp. 29-44.

166 Peter K. Yu, *Op. Cit.,* p. 277.

167 Yifat Nahmias e Maayan Perel, "The Oversight of Content Moderation by AI: impact assessments and their limitations", *in Harvard Journal on Legislation*, n.º 1, Vol. 58, 2021, pp. 145-194.

168 Mirko Forti, *Op. Cit.,* pp. 32/34.

Nesse sentido, Taylor apontou a insuficiência das regras do Regulamento para fins de proteção do titular de dados notadamente no tocante a imprecisões ocorridas no curso do do processo decisório automatizado[169]. Para o autor, seja o direito a explicação (artigos 13.º a 15.º), seja o direito a não ser submetido a decisões automatizadas (artigo 22.º) asseguram um bom nível de qualidade de tratamento de dados, pois, no primeiro caso o dever é de o responsável pelo tratamento genericamente informar as consequências da decisão, mas isso não abrange descrever potenciais imprecisões, muitas vezes sequer conhecidas[170]. No segundo caso, igualmente, pois o titular pode querer consentir com a decisão automatizada, desde que ela esteja atrelada a uma garantia da precisão do algoritmo e da ausência danos em potencial daí decorrentes. O autor faz, ainda, um paralelo entre o dever de transparência do RGPD e o consentimento informado exigido no caso de submissão do paciente a um procedimento médico, em que não basta a informação acerca da natureza e fases do procedimento, tampouco alerta acerca da possibilidade de o tratamento vir a não ser eficaz, mas indispensável a enumeração dos riscos inerentes ao procedimento, mesmo que ele acontença exactamente da forma como programada[171].

Por todas essas peculiaridades da AI e, consequentemente, dos dispositivo de Internet das coisas, sobretudo a amplitude de sua penetrabilidade e as múltiplas áreas em que sua implementação é possível, Nahmias e Perel concluem no sentido de ser impossível a imposição de um único sistema regulatório flexível o suficiente para satisfazer as demandas próprias de cada setor, razão pela qual defendem criação de regras específicas a cada domínio[172].

5.5. OS ALGORITMOS E O DIREITO A SER ESQUECIDO

O artigo 17.º do RGPD apresenta uma prerrogativa do titular de dados que constitui uma das principais inovações do diploma: o direito ao apagamento de dados, também chamado de direito a ser esquecido. Esse direito pode ser exercido por qualquer dos motivos elencados pela lei, entre os quais a retirada do seu consentimento às decisões automatizadas e sua oposição a elas (artigo 17.º, n.º 1, *c)*).

Tal prerrogativa legal tem impacto significativo no funcionamento da Inteligência Artificial, pois o sistema alcança maior eficiência quanto maior seja a base de dados da qual extrai suas decisões. Ou seja, o apagamento de qualquer dado, mesmo que o tratamento não mais interesse ao seu titular

169 Roger Taylor, *Op. Cit.,* pp. 72/73.

170 O exemplo apresentado pelo autor se refere às análises automatizadas de crédito. Cabe ao responsável, pelo direito à informação o dever de informar ao titular a existência da decisão automatizada e possibilidade de aquele crédito ser ou nao negado, sem necessidade de mencionar imprecisões do algoritmo que podem levar a uma decisão injusta.

171 Roger Taylor, *Op. Cit.,* pp. 72/73.

172 Yifat Nahmias e Maayan Perel, *Op. Cit.*, p. 163.

individualmente, interfere no estabelecimento dos padrões pelo dispositivo e na sistemática de funcionamento do algoritmo a ele associado[173].

Outra dificuldade, de ordem eminentemente prática, refere-se à dificuldade de implementação do direito ao apagamento e/ou custos envolvidos no processo[174]. Isso porque, é próprio desse tipo de tecnologia a implementação de mecanismos e medidas contra falhas no sistema suficientes para causar perdas significativas e corrupção dos processos, como por exemplo os *backups* automáticos e a capacidade de acessar versões anteriores do banco de dados. Isso não só é essencial ao bom funcionamento e segurança do sistema, mas também constitui uma obrigação legal decorrente do artigo 32.º do RGPD, principalmente em relação ao n.º 1, *c)*.

Nesse tocante, é mister mencionar já ter o TJUE decidido acerca do direito ao esquecimento – com base em construção jurisprudencial antes mesmo da entrada em vigor do RGPD – no famoso caso, aqui já referido, envolvendo *Google Spain* e a Agência Espanhola de Proteção de dados e Mario Costeja González[175]. Na ocasião o Tribunal já se manifestou sobre o conflito entre direitos fundamentais evidenciado entre o direito do titular à sua vida privada e à proteção de seus dados e o interesse económico do motor de busca, bem como o dos internautas em aceder a informações pessoais através do motor de busca. Ainda, o acórdão, do ponto de vista material, afirma expressamente que o dever de apagamento não induz à necessidade de suprimir totalmente a página dos índices do motor de busca, mas tão somente à desindexação desse resultado à busca pelo nome da pessoa[176]. Por esse motivo, Cabral[177] defende não coincidirem o "direito à não indexação", reconhecido no acórdão, e o "direito a ser esquecido", tal qual expressamente previsto no RGPD, para o autor de modo significativamente mais desenvolvido. De qualquer forma, é oportuno ressaltar que o TJUE traçou limites desse direito ao esquecimento (ou à não indexação) que, longe de absoluto, deve ser exercido em consideração aos demais interesses envolvidos, e em harmonia com os direitos fundamentais de terceiros, sobretudo se pensarmos nas hipóteses em que da confiabilidade do sistema depende a proteção à saúde e, consequentemente, o direito à vida, como nos casos envolvendo dispositivos *e-Health*.

---

173 Mirko Forti, *Op. Cit.*, p. 39.

174 Tiago Sérgio Cabral, *Op. Cit.*, p. 383.

175 Caso *Google Spain* contra AEPD (C-230/14, EU:C:2014:317). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN

176 A esse respeito, destaca-se a análise do GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. Diretrizes para a Execução do Acórdão do Tribunal de Justiça da União Europeia no Processo c-131/12, Google Spain sl e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González. Novembro, 2014. Disponível em https://ec.europa.eu/newsroom/article29/items/667236/en (Consulta em 09.08.2021).

177 Tiago Sérgio Cabral, "Forgetful AI: AI and the Right to Erasure under the GDPR.", *in European Data Protection Law Review*, n.º 3, Vol. 9, 2020, pp. 378-389.

Para Cabral[178], todavia, essa não é uma incompatibilidade incontornável, pois embora os padrões estabelecidos pelo *machine learning* demandem a maior quantidade possível de dados pessoais acumulados, os padrões em si não se referem a nenhuma pessoa em específico, de modo que essas "regras" resultantes dos processamentos dos dados, não podem ser considerados dados pessoais e, por isso, não estão sujeitos ao apagamento. Para ilustrar, o autor apresenta o exemplo de uma aplicação que identifica quando as pessoas que estão posando para uma fotografia se encontram a sorrir e de olhos abertos. Para que o dispositivo "aprenda" a identificar essas circunstâncias, são fornecidas milhares de fotografias de pessoas com variados tipos de sorrisos e cores dos olhos. Da análise de todas essas fotografias (dados pessoais), o algoritmo define padrões que irá utilizar para aferir se as pessoas estão ou não a sorrir. Esses padrões não remetem a nenhuma pessoa e é impossível estabelecer de qual fotografia o sistema extraiu determinada informação, pois o modelo corresponderia à representação de todos os dados pessoais agregados.

Por isso, o autor conclui que a realidade da inteligência artificial pode ser conciliada com as regras do RGPD, cabendo aos desenvolvedores desse tipo de tecnologia ter em conta: a) a necessidade de implementar algoritmos resistentes ao apagamento dos dados, utilizando as estratégia de *privacy by design* e *privacy by defalt*; b) garantir uma volumosa quantidade de dados para diminuir o impacto do apagamento, se possível mediante anonimização; c) evitar tanto quanto possível o tratamento de dados com base no consentimento ou no interesse legítimo, dando preferência para o estabelecimento de uma relação contratual[179].

6. CONCLUSÃO

A noção de privacidade apresenta contornos fluidos que se contraem e se dilatam a depender do contexto histórico e social. Nesse aspeto, a tecnologia sempre exerceu relevante influência no conceito e impulsionou a proteção jurídica do bem. É da evolução da noção de privacidade e do desenvolvimento tecnológico relativo ao processamento de dados que surge o direito à proteção de dados.

Por sua vez, a Internet das Coisas representa a evolução da internet e concretiza realidade antes restrita às obras de ficção científica, inaugurando uma nova era tecnológica e ensejando a demanda por regulamentação dessa atividade. Embora tenhamos realizado um recorte neste estudo para analisar os dispositivos *IoT*, é certo que essa tecnologia está comumente associada à inteligência artificial, operada através de algoritmos e dotada

178 Tiago Sérgio Cabral, *Op. Cit.* p. 385.
179 Tiago Sérgio Cabral, *Op. Cit.,* p. 388.

de *machine leraning*, bem como necessita de uma volumosa quantidade de dados (*Big Data*), muitas vezes armazenada em nuvem (*cloud computing*). Todo esse cenário tecnológico contribui para o desafio da aplicação da legislação aos dispositivos interconectáveis.

Já o Regulamento Europeu de Proteção de Dados, embora recentemente aprovado, surge como resultado da evolução histórica da legislação de proteção de dados pessoais ao logo de décadas e assenta-se, portanto, em conceitos e premissas que remontam a períodos em que o progresso tecnológico alcançava níveis consideravelmente inferiores de automação e dependia quase integralmente da intervenção humana para realização dos processos.

Estabelece-se, então, um aparente paradoxo em que o avanço tecnológico é ao mesmo tempo causa da necessidade por regulamentação do tratamento de dados pelo Estado, mas também sua velocidade pode representar uma obsolescência dessas regras.

Contudo, por todo o exposto neste trabalho, conclui-se que essa contradição é meramente aparente e, se acompanhado de uma interpretação sistemática e atenta ao contexto tecnológico, o RGPD representa um avançado sistema de regras suficiente a garantir a proteção de dados e a privacidade dos titulares, sem impor óbices desproporcionais ao desenvolvimento tecnológico. Mais do que nunca, faz-se necessário dos operadores do direito um olhar para o texto normativo nunca desassociado das peculiaridades de cada realidade tecnológica e sempre mediante a ponderação dos vários interesses e direitos envolvidos. O verdadeiro desafio está exatamente nessa compatibilização entre a estabilidade das regras postas e a ebulição do mundo tecnológico com suas constantes e velozes mudanças.

A eventual defesa da inaplicabilidade do RGPD ao mundo da Internet das Coisas pode resultar em uma total e danosa desproteção dos direitos da personalidade, bem como na construção de um ambiente tecnológico inseguro e lesivo até mesmo ao desenvolvimento enconómico. Igualmente, não nos parece o melhor caminho a defesa de uma mudança constante da lei a reboque das evoluções tecnológicas, sob pena, mais uma vez, de se sacrificar a necessária segurança jurídica.

Assim, entendemos que o Regulamento Geral de Proteção de Dados quando bem interpretado constitui importante ferramenta para a pacificação dos conflitos em relação aos dispositivos de *IoT*, não só por possibilitar o desenvolvimento e aprimoramento da tecnologia, mas por direcioná-los ao fim de garantir o bem-estar das pessoas, tendo como norte os direitos da personalidade atrelados aos interesses económicos.

7. REFERÊNCIAS BIBLIOGRÁFICAS

"Legal Perspectives on the Internet of Things", *in Conferinta Internationala de Drept, Studii Europene si Relatii Internationale*, 2018, disponível em https://heinonline.org/HOL/Page?public=true&handle=hein.journals/cidstue2018&div=55&start_page=523&collection=journals&set_as_cursor=0&men_tab=srchresults (Consulta em 08.08.2021)

Ashton, Kevin, "That 'Internet of Things' Thing", *in RFID Journal,* 2009, disponível em https://www.rfidjournal.com/that-internet-of-things-thing (Consulta em 01.02.2021)

Barbosa, Mafalda Miranda, "Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil.", *in Estudos de Direito do consumidor*, n.º 12, Coimbra, Centro de Direito do Consumo/FDUC, 2017, pp. 75-131.

Betkier, Marcin, *Privacy Online, Law and the Effective Regulation of Online Services*. Cambridge, Intersentia, 2019.

Bioni, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento.* Rio de Janeiro, Forense, 2019.

Brasher, Elizabeth A., "Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation.", *in Columbia Business Law Review*, n.º 1, 2018, pp. 209-253, disponível em https://heinonline.org/HOL/Page?handle=hein.journals/colb2018&id=215&collection=journals&index=# (Consulta em 01.08.2021)

Cabral, Tiago Sérgio, "Forgetful AI: AI and the Right to Erasure under the GDPR.", *in European Data Protection Law Review*, n.º 3, Vol. 9, 2020, pp. 378-389.

Carvalho, Orlando De, *Teoria Geral do Direito Civil,* 3ª ed., Coimbra, Coimbra Editora, 2012.

Comité Económico E Social Europeu, *Parecer sobre "Confiança, privacidade e segurança para os consumidores e as empresas na Internet das coisas (IdC)*" Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018IE1038&qid=1625339548895&from=PT (Consulta em 01.07.2021)

Comité Europeu De Proteção De Dados (CEPD), *Diretrizes 3/2018 sobre o âmbito de aplicação territorial do RGPD (artigo 3.º)*, versão 2.0, de 12/11/2019. Disponível em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf (Consulta em 01.08.2021)

Cordeiro, António Barreto Menezes, "O consentimento do titular dos dados no RGPD., *in FinTech: desafios da tecnologia financeira.* coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte, Vol. 2, Almedina, Coimbra, 2017, pp. 33-56.

Cordeiro, António Barreto Menezes, *Direito da Proteção de Dados*: à luz do RGPD e da Lei nº 58/2019. Coimbra, Almedina. 2020.

Corôa, Marília De Mello E Silva, *O Mercado De Dados: Estrutura, Funcionamento e o Reflexo do RGPD no Novo Mercado à Base De Dados Pessoais*. Dissertação (Mestrado em Ciências Jurídico-civilísticas) Faculdade de Direito da Universidade do Porto, Porto, 2020.

Correia, Victor. *Sobre a Privacidade*. Sinapsis Editores, 2016.

Cremona, Marise, *New Technologies and EU Law*. Oxford, Oxford University Press, 2017.

De Conca, Silvia, "Between a rock and a hard place: Owners of smart speakers and joint control", *in SCRIPTed*, n.º 2, Vol. 17, 2020, pp. 238-268.

Dias, Carlos André Ferreira, *A Privacidade na era da Internet das Coisas: direiros de personalidades e proteção de dados.* Dissertação (Mestrado em Ciências Jurídico-civilísticas) Faculdade de Direito da Universidade do Porto, Porto, 2019.

-*Diretrizes para a Execução do Acórdão do TJUE no Processo c-131/12, Google Spain sl e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Novembro, 2014, disponível em https://ec.europa.eu/news-room/article29/items/667236/en (Consulta em 09.08.2021).

Elvy, Stacy-Ann, "Contracting in the age of the internet of things: article of the ucc and beyond.", *in Hofstra Law Review*, nº 3, Vol. 44, 2016, disponível em https://heinonline.org/HOL/Page?public=true&handle=hein.journals/hofl-r44&div=40&start_page=839&collection=journals&set_as_cursor=0&men_tab=srchresults (Consulta em 01.08.2021)

Fabiano, Nicola, "Internet of Things and the Legal Issues Related to the Data Protection Law according to the New European General Data Protection Regulation.", *in Athens Journal of Law*, Vol. 3., 2017, pp. 201-214.

Forti, Mirko, "The Deployment of Artificial Intelligence Tools in the Health Sector: Privacy Concerns and Regulatory Answers within the GDPR.", *in European Journal of Legal Studies*, n.º, 1, Vol. 13, 2021, pp. 29-44.

Frias, Hélder, "A Internet de Coisas (IoT) e o Mercado Segurador.", *in FinTech: desafios da tecnologia financeira.* coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte, Vol. 1. Almedina, Coimbra, 2017, pp. 219-233.

Goldstein, Ken, "Cyber Beware: Iot Technology Growing Explosively.", *in International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel*, n.º 6, Vol. 3, 2019, disponível em https://heinonline.org/HOL/P?h=hein.journals/idpp3&i=131 (Consulta em 01.08.2021).

Grupo De Trabalho Do Artigo 29.º Para A Proteção De Dados.

Guimarães, Maria Raquel e Redinha, Maria Regina, "Through the Keyhole: Privacy in COVID-19 Times — A Portuguese Approach." *in Intersentia Online, 2020*, disponível em https://www.intersentiaonline.com/publication/coronavirus-and-the-law-in-europe/2 (Consulta em 01.08.2021)

Kamarinou, Dimitra; Millard, Christopher; e Singh, Jatinder, "Machine Learning with Personal Data", *in Data Protection and Privacy: The Age pf Intelligent Machines,* Ronald Leenes, *et al*., Oxford, Hart, 2017, pp. 89-112.

La Diega, Guido Noto, "Internet of things and patents: Towards the iot patent wars.", *in Journal of Commercial and Intellectual Property Law*, n.º 2, Vol. 3, 2017, disponível em https://heinonline.org/HOL/Page?handle=hein.journals/tfm2017&id=223&collection=journals&index= (Consulta em 01.08.2021).

Luger, Ewa e Rosner, Gilad, "Considering the Privacy Design Issues Arising from Conversation as a Platform", *in Data Protection and Privacy: The Age pf Intelligent Machines,* Ronald Leenes, *et al*., Oxford, Hart, 2017, pp. 193-211.

Magrani, Eduardo, *A Internet das Coisas*, Rio de janeiro, FGV Editora, 2018.

Nahmias, Yifat. e Perel, Maayan, "The Oversight of Content Moderation by AI: impact assessments and their limitations", *in Harvard Journal on Legislation*, n.º 1, Vol. 58, 2021, pp. 145-194.

Odreasova, Eva, "Personality Rights in Different European Legal Systems: Privacy, Dignity, Honour and Reputation." *in The Legal Protection of ersonality Rights: Chinese and European perspectives,* OLIPHANT, Ken; PINGHUA, Zhang; e LEI, Chen. Leiden. Brill, 2018, pp. 24-70.

Oliveira, Madalena Perestrelo de, "Definição de Perfis e Decisões Automatizadas no Regulamento Geral sobre a Proteção de Dados", *in FinTech: desafios da tecnologia financeira*. coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte, Vol. 2, Almedina, Coimbra, 2017. pp. 61-88.

-*Opinion 3/2013 on purpose limitation.* Abril, 2013. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (Consulta em 01.07.2021)

-*Opinion 8/2014 on the on Recent Developments on the Internet of Things*. Setembro, 2014, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (Consulta em 01.07.2021)

-*Orientações relativas à transparência na aceção do Regulamento 2016/679*. Novembro, 2017. Disponível em https://www.uc.pt/protecao-de-dados/suporte/20180411_orientacoes_relativas_a_transparencia_wp260_rev01 (Consulta em 02.08.2021)

-*Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*. Novembro, 2017, disponível em file:///C:/Users/User/Downloads/20180416_article_29_wp_guidelines_on_consent_publish_09A6854F-F638-8898-7A-0543CE0857250F_51030.pdf (Consulta em 02.08.2021)

-*Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*. Outubro, 2017. Rev. Fevereiro, 2018, disponível em file:///C:/Users/User/Downloads/guideline%20decis%C3%B5es%20automatizadas%20e%20profilling.pdf (Consulta em 05.08.2021)

Pagallo, Ugo, "The legal challenges of Big Data: putting secondary rules first in the field of EU Data Protection.", *in European Data Protection Law Review* (EDPL), 2017, n.º 1, Vol. 3, pp.36-46.

Pagallo, Ugo; Massimo, Durante, e Monteleone, Shara. "Whats is New with the Internet of Things in Privacy and Data Protection? For Legal Chalenges on Sharing and Control in IoT.", *in Data Protection and Privacy: (In)visibilities and Infrastructures*, Ronald Leenes, *et al*., Cham, Springer, 2017. (Law, governance and technology series), pp. 59-78.

Peppet, Scott R, "Freedom of Contract in Augmented Reality" *in Research Handbook on the Law of Virtual and Augmented Reality*, Chelteham, Edward Elgar, 2020, p. 609/635.

Peppet, Scott R., "Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent.", *in Texas Law Review*, 2014.

Pinheiro, Alexandre Sousa, *et al, Comentário ao regulamento geral de proteção de dados*, Coimbra, Almedina, 2018.

Pinheiro, Alexandre Sousa, *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*. Lisboa, AAFDL, 2015.

Pinto, Paulo Mota, *Direitos de Personalidade e Direitos Fundamentais: estudos*. Coimbra, Gestlegal, 2018.

Rouvroy, Antoinette, "Of Data and Men: Fundamental Rights and Freedoms in a World of Big Data", *in Council of Europe, Directorate General of Human Rights and Rule of Law*, 2016. Disponível em https://rm.coe.int/16806a6020 (Consulta em 01.08.2021)

Sarmento E Castro, Catarina, "40 anos de "Utilização da Informática" — O artigo 35.º da Constituição da República Portuguesa.", *in Revista e-Pública*, n.º 3, Vol. 3, 2016, pp. 42/66. Disponível em https://www.e-publica.pt/volumes/v3n3a04.html (Consulta em 01.08.2021)

Siegel, Jeremy, "When the Internet of Things Flounders: Looking into GDPR-Esque Security Standards for IoT Devices in the United States from the Consumers' Perspective.", *in Journal of High Technology Law*, n.º 1, Vol. 20, 2020, pp. 189-229, disponível em https://heinonline.org/HOL/Page?handle=hein.journals/jhtl20&id=189&collection=journals&index= (Consulta em 01.04.2020)

Solove, Daniel J., *The Digital Person.* New York and London. New York University Press, 2004.

Taylor, Roger, "No privacy without Transparency", *in Data Protection and Privacy: The Age of Intelligent Machines.* Ronald Leenes, *et al*. Oxford, Hart, 2017, pp. 63-85.

Tomé, Herminia Campuzano, Vida Privada y Datos Personales: Su Protección Jurídica Frente a La Sociedad de la Información. Madrid, Tecnos, 2000.

Warren, Samuel D. e Brandeis, Louis D., "The Right to Privacy.", *in Harvard Law Review*, n.º 5, Vol. IV, 1890. pp. 193-220.

Yu, Peter K., "Beyond Transparency and Accountability: Three additional features algorithm designers should build into intelligent platforms.", *in Northeastern University Law Review*, n.º 1, Vol. 13, 2021, pp. 263-296.

Zarsky, Tal Z., "Desperately Seeking Solutions: Using implementation-based solutions for the troubles of information privacy in the age of data mining and the internet society.", *in Maine Law Review*, n.º 1, Vol. 56, 2004, pp. 13-60, disponível em:https://heinonline.org/HOL/Page?public=true&handle=hein.journals/maine56&div=7&start_page=13&collection=journals&set_as_cursor=0&men_tab=srchresults (Consulta em 16.08.2021)

Zarsky, Tal Z., "Incompatible: The GDPR in the Age of Big Data.", *in Seton Hall Law Review*, n.º 4, Vol. 47, 2017. pp. 995-1020, *disponível em* https://heinonline.org/HOL/P?h=hein.journals/shlr47&i=1019 (Consulta em 30.7.2021)

RESERVA DA VIDA PRIVADA DOS TRABALHADORES: DISPONIBILIDADE E EFETIVAÇÃO

Liliana Catarina Fortuna Cruz

lilianacatarinafortunacruz@gmail.com

Resumo: A presente dissertação tem por objeto o direito à reserva da vida privada no âmbito da relação laboral, com especial ênfase na disponibilidade do direito pelo seu titular e nas diversas formas de violação do mesmo por parte da entidade empregadora.

Pese embora se trate de um direito inerente a todas as pessoas, com reconhecimento na Lei Fundamental e afirmação na jurisprudência do Tribunal Constitucional, só há bem pouco tempo é que o direito à reserva da vida privada começou a ter ressonância no direito do trabalho.

Assim, iniciamos este estudo com uma análise das principais caraterísticas do direito à reserva da vida privada, na sua dimensão constitucional e enquanto direito de personalidade, seguida por uma breve referência à evolução conceptual e social que o mesmo atravessou nos últimos dois séculos, motivada sobretudo pelos desenvolvimentos tecnológicos e da sociedade de informação.

Após esse enquadramento, procuraremos enunciar em traços gerais o reconhecimento do direito à reserva da vida privada no direito do trabalho e, bem assim, as principais vicissitudes que o mesmo enfrenta na relação laboral, em virtude do desequilíbrio contratual entre as partes, desde o momento da contratação até à cessação do contrato.

Porém, a apreciação crítica deste trabalho recairá sobre a possibilidade de disponibilidade do direito à reserva da vida privada por parte dos trabalhadores, em especial através do consentimento, bem como sobre os mecanismos de efetivação existentes para reagir às constantes violações desse direito levadas a cabo pelas entidades patronais.

Para terminar, faremos uma resenha jurisprudencial, de forma a demonstrar como o Tribunal Europeu dos Direitos do Homem e os tribunais portugueses têm decidido as questões relativas ao direito à reserva da vida privada, sobretudo quando estão em causa litígios laborais.

Palavras-chave: Reserva da vida privada; Direito do trabalho; Desequilíbrio contratual; Disponibilidade; Consentimento

Abstract: The purpose of this dissertation is to examine the right to privacy within the scope of the employment relationship, with special emphasis on the availability of this right to privacy by its holder and the various forms that violation of this privacy by the employer may take.

Even though it is a right inherent to everyone, with recognition in the Portuguese Constitution and in the jurisprudence of the Portuguese Constitutional Court, it is only recently that the right to privacy has begun to gain prominence in labour law.

Thus, we chose to start this study with an analysis of the main characteristics of the right to privacy in its constitutional dimension and as a personality right; brief reference is made to the conceptual and social evolution of this right over the last two centuries, motivated mainly by recent technological developments and the advent of the information society.

Following on from this background we seek to outline the recognition of the right to the protection of private life in labour law, as well as the main vicissitudes which it faces in the employment relationship. The contractual unbalance existing between the parties, from the moment of contracting until the termination of the contract is examined.

However, the critical appraisal of this work will focus on the potential availability of the right to privacy by employees, in particular through consent, as well as on the existing enforcement mechanisms to react to the constant violations of this right to privacy by employers.

Finally, we will make a case law overview, to demonstrate how the European Court of Human Rights and the Portuguese courts have decided the issues related to the right to privacy, especially when labour disputes are at stake.

Keywords: Keywords: Privacy; Labour law; Contractual imbalance; Availability; Consent

1. INTRODUÇÃO

Se outrora a principal preocupação dos juslaboralistas era a de impedir que as entidades empregadoras pudessem sujeitar os seus trabalhadores a condições de trabalho degradantes, a jornadas de trabalho excessivas e a salários muito baixos, o novo desafio que hoje se coloca é o de garantir na relação laboral a manutenção dos direitos de personalidade que cada cidadão possui enquanto ser humano. Aliás, ambas as preocupações estão interligadas e têm um propósito comum, que é o de garantir a dignidade dos trabalhadores enquanto pessoas. Para o efeito, torna-se necessário protegê-los de eventuais ofensas encetadas pelos empregadores e, simultaneamente, acautelar as situações nas quais são os próprios trabalhadores que de forma voluntária abdicam ou restringem os seus direitos.

Assim, com o presente trabalho, procuraremos trazer à discussão a importância do direito à reserva da vida privada na relação laboral, numa altura em que os meios tecnológicos colocados à disposição das entidades empregadoras constituem ameaças severas e muitas vezes ocultas a esse direito e em que uma parte significativa dos trabalhadores tolera intromissões na sua vida privada, sem que seja essa efetivamente a sua vontade.

Se, até ao ano de 2020, a visibilidade e a atenção dogmática conferidas ao direito à reserva da vida por grande parte dos trabalhadores eram parcas, a verdade é que o contexto da Covid-19 permitiu alertar para questões que já vinham a acontecer, mas que se tornaram mais evidentes em função das circunstâncias vividas[1], levando a que vários trabalhadores se sentissem lesados e questionassem o alcance deste direito e as formas através das quais poderiam reagir a possíveis violações do mesmo. Assim, podemos dizer que a pandemia que se iniciou em 2020 reacendeu novamente o debate em torno do direito à reserva da vida privada, quer numa perspectiva social e de saúde pública, quer no seio das relações de trabalho.

Por esse motivo, neste trabalho iremos recuperar alguns conceitos e ideias já desenvolvidas sobre o direito à reserva da vida privada, para depois serem problematizadas temáticas mais atuais. Nesse sentido, procuraremos responder às seguintes questões: Em que consiste o direito à reserva da vida privada? Que sentido tem reconhecer este direito na relação laboral? O direito à reserva da vida privada está na disponibilidade das partes e, mais concretamente, dos trabalhadores? Quais os meios de reação face a viola-

[1] Falamos de situações como: a solicitação pelas entidades empregadoras de dados de saúde dos trabalhadores e dos seus familiares, sobretudo através do consentimento; a colocação de programas ocultos nos instrumentos de trabalho facultados aos trabalhadores que ficaram em teletrabalho; o recurso a videoconferências para realização de reuniões à distância, muitas vezes com a obrigatoriedade de manter a câmera ligada; a requisição de informações sobre os meios de comunicação e outras condições habitacionais dos trabalhadores; entre outras.

ções deste direito na relação laboral? Para tal, começaremos por delimitar o conceito e o âmbito do direito à reserva da vida privada, de forma a evidenciar as suas principais caraterísticas e a forma como vem sendo tratado na relação laboral, através da análise da sua evolução doutrinal, legislativa e jurisprudencial. Abordados esses aspetos, direcionaremos a nossa atenção para algumas formas de afetação desse direito, quer por parte da entidade empregadora (violações do direito) quer por parte dos próprios trabalhadores (disponibilidade)[2].

2. O DIREITO À RESERVA DA VIDA PRIVADA

2.1. DIGNIDADE E PERSONALIDADE

Antes de mais, é importante enquadrar a reserva da vida privada no seio dos direitos fundamentais, mais concretamente como sendo um dos DLG's aos quais a CRP confere especial proteção[3]. Esses direitos encontram-se nos arts. 24º a 57º da CRP e têm como fim último a proteção da dignidade da pessoa humana, consagrada no art. 1º da Constituição.

A proteção conferida à reserva da vida privada surge no art. 26º, nº 1 da CRP, sob a epígrafe *"outros direitos pessoais"*[4], muito embora também os artigos 32º, nº 8, 34º, nº 1, 35º e 268º, nº 2, todos da CRP, representem concretizações deste direito.

A especial tutela conferida aos DLG's constitui um regime geral específico, previsto nos artigos 18º a 22º, bem como nos artigos 168º, nº 1, *al. b)*, 272º, nº 3 e 290º, *al. d),* todos da CRP, do qual resulta uma preocupação acrescida com este núcleo de direitos quando comparada com a proteção prevista para os outros direitos fundamentais.

---

[2] Apesar de o tema deste trabalho contender com várias outras questões, tais como as publicações dos trabalhadores ou candidatos a emprego nas redes sociais, o tratamento de dados pessoais (em especial dos dados relativos à saúde), a utilização de plataformas digitais, o teletrabalho, o uso do correio eletrónico, entre outras, não iremos cuidar delas aqui, em virtude dos limites de tempo e espaço inerentes a este trabalho.

[3] Como refere VIEIRA DE ANDRADE, os DLG's podem ser entendidos como um conjunto de direitos intrínsecos à pessoa humana, dos quais decorrem todos os outros. (Cfr. José Carlos Vieira De Andrade, *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, Coimbra, Almedina, 1987, Reimpressão, p. 25)

[4] Este enquadramento corrobora o defendido por Orlando de Carvalho nos seus ensinamentos, no sentido de o direito à reserva da vida privada consubstanciar um dos círculos de projeção vital da inviolabilidade pessoal. Cfr. Maria Regina Redinha, "*Da proteção da personalidade no Código do Trabalho"*, *in Para Jorge Leite - Escritos Jurídico-Laborais,* coord. João Reis, Leal Amado, Liberal Fernandes E Regina Redinha, vol. I, Coimbra Editora, 2014, p. 824.

Esse regime determina que os DLG's gozam de aplicabilidade direta e imediata e que apenas podem ser restringidos se houver um motivo de força maior, que supere o teste de proporcionalidade previsto no art. 18º, nº 2 da CRP, nas suas três vertentes: necessidade; adequação; e proporcionalidade em sentido estrito.

Conforme refere Vieira de Andrade[5], os direitos fundamentais são considerados "*direitos absolutos, imutáveis e intemporais, inerentes à qualidade de homem dos seus titulares"*, dirigindo-se quer ao Estado quer a entidades privadas. Assim, embora noutros tempos a necessidade mais premente fosse a de proteger os cidadãos perante o Estado[6], atualmente reconhece-se que a eficácia dos direitos fundamentais vai muito para além disso, impondo-se igualmente aos particulares entre si, em especial nas relações privadas em que as partes se encontram em condições de assimetria estatutária, como acontece na relação laboral[7].

Apesar de o art. 3.º, nºs 2 e 3, da CRP determinar a sujeição de todas as entidades, quer públicas quer privadas, ao cumprimento dos direitos fundamentais, a eficácia dos direitos fundamentais entre particulares não é consensual. Não obstante tal eficácia resultar de forma expressa do nº 1 do art. 18º da CRP, uma parte da doutrina vem defendendo que os direitos fundamentais têm eficácia direta nas relações entre particulares[8], ao passo que outros autores sublinham o papel de defesa da liberdade assumido pelos direitos fundamentais, considerando que uma eficácia dos mesmos no direito privado retiraria sentido aos princípios da autonomia privada e da liberdade contratual que estão na génese das relações entre privados[9].

Não descurando a razão de ser da controvérsia, a solução adequada parece-nos ser a tese segundo a qual os direitos fundamentais vinculam os particulares quando se trate de uma relação de direito privado na qual as partes têm posições desiguais, levando a que uma exerça sobre a outra um poder semelhante ao do Estado[10]. Aliás, é esse o ponto de encontro das muitas teorias que foram surgindo, na medida em que se foi gradualmen-

---

5 Cfr. José Carlos Vieira De Andrade, *Os Direitos Fundamentais...*, p. 14.

6 Fala-se, a esse respeito, de uma eficácia externa dos direitos fundamentais, que a doutrina alemã designa de *Drittwirkung der Grundrechte*.

7 É precisamente com base nessa preocupação que a generalidade da doutrina tende, hoje, a admitir a eficácia horizontal dos direitos fundamentais. Cfr. José João Nunes Abrantes, *Contrato de Trabalho e Direitos Fundamentais*, Coimbra Editora, 2005, ISBN 972-32-1330-3, p. 15-20.

8 Nesse sentido, v. J.J. Gomes Canotilho; Vital Moreira, *Constituição da República Portuguesa Anotada, Arts. 1º a 107º,* vol. I, 4ª ed. revista, Coimbra Editora, 2007, ISBN 978-972-32-1462-8, p. 384-386, anotação IV ao art. 18º.

9 Dos quais se destaca GUNTER DURING, conforme refere TERESA COELHO MOREIRA. (Cfr. Teresa Alexandra Coelho Moreira, *Da Esfera Privada do Trabalhador e o Controlo do Empregador*, Studia Iuridica 78, Coimbra Editora, 2004, ISBN 972-32-1228-5, p. 50)

10 É o que defendem, por exemplo, VIEIRA DE ANDRADE (Cfr. José Carlos Vieira De Andrade, *Os Direitos Fundamentais...*, p. 285-287) e MOTA PINTO (Cfr. Paulo Mota Pinto,

te reconhecendo a necessidade de proteger os indivíduos contra ofensas à sua dignidade, embora mantendo presente a necessidade de salvaguardar a autonomia privada e a liberdade negocial caraterísticas do direito privado.

Assim, a reserva da vida privada apresenta-se atualmente como um direito fundamental, de aplicabilidade direta e imediata, tendo como sujeitos passivos o Estado e as demais entidades públicas e ainda as entidades privadas que exerçam algum poder económico ou social sobre os indivíduos, o que permite aos trabalhadores invocar o seu direito à reserva da vida privada perante a atuação dos seus empregadores.

Por outro lado, os direitos fundamentais têm projeção no direito privado através da concretização que deles é feita por normas de direito privado, em especial pelos direitos da personalidade, que estão previstos no Título II do Código Civil[11].

Apesar de terem origem no direito romano, os direitos da personalidade só se desenvolveram e adquiriram a importância que hoje lhes reconhecemos ao longo do séc. XIX e, mais acentuadamente, no séc. XX, após a Segunda Guerra Mundial[12].

Os direitos de personalidade são direitos pessoais, intrínsecos à própria pessoa, que conferem proteção e permitem o desenvolvimento da personalidade de cada um, na medida em que concebem a pessoa humana «como espaço de exclusão, por ser pressuposto essencial da sua existência a não interferência prejudicial dos outros no que ela é»[13].

Nesse sentido, os direitos de personalidade concretizam os preceitos constitucionais no direito privado e caraterizam-se por serem direitos gerais, absolutos, não patrimoniais, irrenunciáveis e parcialmente disponíveis[14], cujo fim último é a tutela da personalidade humana, nas diferentes vertentes que a compõem[15].

O art. 70º do CC, que inicia o leque de direitos de personalidade consagrado nesse diploma, tem sido entendido por vários autores, entre os quais Paulo Mota Pinto, R. Capelo Sousa e Heinrich Horster, como traduzindo um direito geral de personalidade, que apenas deverá funcionar em *utima ratio*, isto é, se

Direitos de Personalidade e Direitos Fundamentais: Estudos, Coimbra, Gestlegal, 2018, ISBN 978-989-54076-3-7, p. 111)

11 Cfr. Paulo Mota Pinto, *Direitos de Personalidade*..., p. 98, 327 e 328.

12 Sobre a origem e a evolução dos direitos de personalidade, v. António menezes cordeiro, *Direito do Trabalho*, vol. I: Direito europeu. Dogmática geral. Direito coletivo, Coimbra, Almedina, 2018, ISBN 978-972-40-7684-3, p. 466-479.

13 Cfr. Diogo leite de campos, *Lições de direitos de personalidade*, 2ª ed. (reimpressão), Separata do vol. 66 (1990) do Boletim da Faculdade de Direito da Universidade de Coimbra, Coimbra, 1995, p. 11.

14 Para uma análise mais detalhada de cada uma destas caraterísticas, v. António menezes cordeiro, *Direito do Trabalho*..., p. 506-510.

15 Cfr. Paulo mota pinto, *O Direito à Reserva Sobre a Intimidade da Vida Privada*, Coimbra, Faculdade de Direito da Universidade de Coimbra, Sep. do Boletim da Faculdade de Direito, vol. 69, 1993, p. 481-489.

os direitos de personalidade específicos não permitirem tutelar uma determinada dimensão da personalidade da pessoa humana[16]. Por sua vez, o art. 80º do CC, que consagra o direito à reserva da vida privada, constitui um direito especial de personalidade, sobre o qual nos debruçaremos adiante.

2.2. EVOLUÇÃO CONCEPTUAL

Apesar da crescente importância que o direito à reserva da vida privada tem adquirido nos últimos anos a nível internacional e nacional, tal evolução é recente e motivada sobretudo pelo progresso tecnológico e pela globalização, que fizeram surgir novos direitos, mas também novas formas de atentar contra esses direitos.

Até ao século XVIII, o ser humano vivia de forma pública, sendo a sua vida pessoal e familiar conhecida por todos[17]. O direito à privacidade não existia, nem era sequer concebível. Contudo, se remontarmos ao final do séc. XIX, identificamos já alguns autores que defendiam a necessidade de proteger a vida privada, em virtude dos desenvolvimentos tecnológicos que se verificavam na altura, embora com base em ofensas muito diferentes daquelas que os avanços tecnológicos e a sociedade de informação viriam a potenciar.

Aliás, quando se procura situar o início da discussão em torno deste direito, a doutrina dos diferentes países tende a apontar o artigo *"The Right to Privacy"* de Samuel D. Warren e Louis Brandeis, como tendo sido o ponto de partida para o surgimento do direito à privacidade, cujo objetivo primordial era, à época, proteger da imprensa a vida privada das pessoas[18].

Com o decorrer do tempo e o desenvolvimento tecnológico, muitos autores, sobretudo nos EUA, procuraram definir "privacidade" através de diversas perspetivas (filosófica, política, sociológica ou psicológica), com o intuito de esclarecer o interesse subjacente ao bem jurídico "inviolabilidade pessoal", entendido este como um espaço próprio e restrito do "eu" face aos outros, que permite a cada pessoa ter uma dimensão individual resguardada da sociedade.

Porém, na Europa Continental, só no final da II Guerra Mundial é que se começou a atribuir importância ao direito à reserva da vida privada, assistindo-se na segunda metade do séc. XX à consagração do mesmo em importantes fontes internacionais, designadamente na Convenção Europeia dos Direitos do Homem (art. 8º), na Declaração Universal dos Direitos Humanos (art. 12º) e no Pacto Internacional sobre Direitos Civis e Políticos (art. 17º).

---

16 Cfr. Teresa alexandra coelho moreira, *Da Esfera Privada do Trabalhador…*, p. 129-132.

17 Cfr. Diogo leite de campOS, *Lições de direitos...,* p. 96.

18 O direito à reserva da vida privada aí consagrado reportava-se, de certa forma, a um direito à solidão, que os autores designaram de "*right to be let alone*", uma expressão do juiz THOMAS COOLEY, que significava que cada indivíduo possui um núcleo só seu, onde não se admitem intromissões externas. Cfr. Samuel D. Warren e Louis Brandeis, *The Right to Privacy*, *Harvard Law Review*, vol. 4, no. 5, Dec. 15. 1890 [Cons. 17 mar. 2021] Disponível em <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf >, p. 195.

Paralelamente a esta evolução social e legislativa, verificou-se também um ponto de viragem na jurisprudência do Tribunal de Justiça da União Europeia quando, no Acórdão de 13 de maio de 2014 (*Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos e Mario Costeja González*)[19] foi reconhecido o direito ao esquecimento. Este Acórdão, que diz respeito, essencialmente, ao tratamento de dados pessoais e à possibilidade de o titular dos dados controlar a livre circulação dos mesmos, constitui um marco importante na evolução do direito à reserva da vida privada, na medida em que veio atribuir ao titular dos dados o direito de os controlar, decidindo quando, como e quem pode utilizar os seus dados[20]. Com tal decisão jurisprudencial, assinalou-se o princípio de um novo tempo de elaboração dogmática, com a qual se procurou reconhecer e atribuir aos titulares das informações o domínio sobre as mesmas.

Esta preocupação da União Europeia consagrar e proteger o direito à reserva da vida privada acabou por ter repercussões nos diferentes ordenamentos jurídicos dos Estados Membros que, em maior ou menor medida, foram adotando disposições nacionais no sentido de proteger e concretizar o direito à reserva da vida privada ou o direito à privacidade[21], com o objetivo de garantir a cada pessoa um espaço de livre desenvolvimento da sua personalidade, no qual as informações que lhe dizem respeito deixem de circular livremente na imprensa ou sejam difundidas através das novas tecnologias de informação.

Em Portugal, antes da Constituição de 1976, praticamente não existiam referências à reserva da vida privada, mas apenas o reconhecimento dos direitos à inviolabilidade do domicílio e da correspondência. Assim, foi no Acórdão nº 128/92, de 24 de julho de 1992, que o Tribunal Constitucional definiu, pela primeira vez, o conteúdo do direito à reserva sobre a intimidade da vida privada, como sendo o «direito de cada um a ver protegido o espaço interior ou familiar da pessoa ou do seu lar contra intromissões alheias»[22].

Em primeiro lugar, importa referir que, apesar de alguma doutrina diferenciar as terminologias "privacidade" e "vida privada", considerando o primeiro conceito mais abrangente do que o segundo[23], neste trabalho, tomá-las-emos como equivalentes, uma vez que se trata de uma problematização inci-

---

[19] Cfr. Acórdão do Tribunal de Justiça (Grande Secção) [Cons. 16 mai. 2021] Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62012CJ0131&from=PT>.

[20] Apesar de este Acórdão suscitar inúmeras questões inovadoras ao nível da proteção de dados no mundo digital, não iremos tratar delas neste trabalho, pois as mesmas só indiretamente se relacionam com os temas que aqui iremos abordar.

[21] Para uma análise da evolução do direito à reserva da vida privada no direito comunitário, v. Teresa Alexandra Coelho Moreira, *Da Esfera Privada do Trabalhador…*, p. 73-104.

[22] Cfr. Paulo Mota Pinto, *Direitos de Personalidade...*, p. 597-601.

[23] A título de exemplo, DIOGO LEITE DE CAMPOS refere que «o direito à privacidade não se resume ao «direito à intimidade da vida privada» confundido com a intimidade do espaço familiar, da casa de morada de família». (Cfr. Diogo Leite De Campos, *Lições de direitos...*, p. 97)

dental para a análise que pretendemos empreender. Além disso, a nosso ver, "privacidade" e "reserva da vida privada" são realidades incidentes sobre o mesmo bem jurídico, sem prejuízo das inúmeras perspetivas que podem ser apontadas para as analisar e compreender. Assim, e à semelhança daquilo que tem vindo a ser feito por alguns autores, faremos alusão à privacidade e à reserva da vida privada como sinónimos[24].

Em segundo lugar, e apesar da abundante doutrina existente em torno de ambos os conceitos, não aderimos à distinção entre "intimidade da vida privada" e "vida privada"[25], pois, como Gomes Canotilho e Vital Moreira[26], consideramos que tal delimitação carece de sentido prático, uma vez que a designação "reserva da vida privada" tem em vista proteger uma série de informações intimamente ligadas à pessoa humana, sem prejuízo de poder incluir outras que se relacionem, por exemplo, com a vida profissional.

Por esse motivo, entendemos que quer a designação "intimidade da vida privada" quer a designação "vida privada", têm o mesmo fim, que é o de proteger as informações que os indivíduos querem guardar para si mesmos ou partilhar apenas com um restrito círculo de pessoas, pelo que não deve existir uma diferenciação na utilização de uma e outra expressão[27].

2.3. ÂMBITO DE PROTEÇÃO

De modo a compreendermos melhor o conceito de vida privada, torna-se necessário contrapor-lhe o conceito de vida pública. Esta última diz respeito à vida social, que pode ser partilhada com o público ou que lhe é acessível. Pelo contrário, a vida privada abrange aspetos relativos ao domicílio; à vida pessoal e familiar; à vida conjugal, amorosa e afetiva das pessoas; à correspondência em formato de papel ou digital; ao telemóvel e às conversas escritas ou orais; à identidade da pessoa; aos dados de saúde; a eventos privados; a entradas e saídas do lar; a encontros com amigos e familiares; a lembranças, escritos e diários; a informações sobre a vida patrimonial e financeira; entre outros[28]. Secundando Menezes Cordeiro, podemos dizer que a vida privada inclui tudo o que não é público, profissional ou social[29].

---

[24] Entendimento já seguido por MARIA REGINA REDINHA e MARIA RAQUEL GUIMARÃES. (Cfr. Maria Regina Redinha e Maria Raquel Guimarães, "*O uso do correio eletrónico no local de trabalho - Algumas reflexões*", *in Estudos em homenagem ao Professor Doutor Jorge Ribeiro de Faria*, 2003, nota 12.)

[25] A propósito desta distinção, veja-se por exemplo Paulo Mota Pinto, *O Direito à Reserva…,* p.530-534.

[26] Cfr. J.J. Gomes Canotilho; Vital Moreira, *Constituição…*, p. 468.

[27] Aliás, o próprio Tribunal Constitucional adota diferentes denominações, sem distinguir entre "intimidade da vida privada" (Acórdão nº 128/92), "esfera privada ou íntima" e "privacidade" (Acórdão nº 470/96).

[28] Cfr. Paulo Mota Pinto, *O Direito à Reserva…*, p. 527-529.

[29] Cfr. António Menezes Cordeiro, *Direito do Trabalho...*, p. 556.

Contudo, a questão que se coloca é a de saber como podemos distinguir a vida privada da vida pública, isto é, quais os critérios que nos permitem aferir se estamos perante informações que integram um campo ou o outro.

Alguns critérios foram sendo apontados na doutrina para operar esta diferenciação, tais como um critério espacial, de acordo com o qual a inserção de determinados dados das pessoas na vida pública ou na vida privada dependia se estes ocorriam ou diziam respeito a um local público ou a um local privado, respetivamente. Como locais privados eram apontados a casa e o carro, ao passo que a via pública, o local de trabalho, uma cabine telefónica, os edifícios públicos e os jardins, entre outros espaços eram entendidos como lugares públicos. Porém, essa tese foi rapidamente desconstruída, quando se percebeu que «alguns episódios da vida privada que devem ser objeto de tutela podem desenrolar-se em lugares públicos»[30], levando a que o critério espacial não seja suficiente para esta distinção. Assim, surgiram outros critérios, tais como averiguar quais as pessoas envolvidas, saber se os factos são verdadeiros ou falsos e ainda a titularidade dos objetos em causa.

Ainda hoje o conceito de reserva de vida privada não tem um objeto estanque, sendo antes um conceito evolutivo, que varia e adquire novos contornos em função das circunstâncias, pelo que não pode ser analisado com base em ideias pré-definidas ou atendendo a um único critério. Pelo contrário, e secundando Teresa Moreira[31], a reserva da vida privada deve ser entendida como um conceito aberto, onde cabem as mais variadas informações que o titular do direito pretende resguardar de determinadas pessoas ou da sociedade em geral.

Porém, tal versatilidade do conceito não significa a impossibilidade de delimitar o seu âmbito de proteção, concretizando a tutela conferida pelo mesmo para, a partir daí, se conseguir compreender se, numa situação específica, o titular do direito pode invocá-lo contra determinada atuação ou se, pelo contrário, se trata de uma situação que fica fora do âmbito de proteção do direito à reserva da vida privada, o que se procurará fazer de seguida.

No Acórdão do TC nº 128/92, de 24/07/1992, pode ler-se que *«este direito a uma esfera própria e inviolável, onde ninguém deve poder penetrar sem autorização do respetivo titular, compreende: a) a autonomia, ou seja, o direito a ser o próprio a regular, livre de ingerências estatais e sociais, essa esfera de intimidade; b) o direito a não ver difundido o que é próprio dessa esfera de intimidade, a não ser mediante autorização do interessado»*[32].

---

30 Cfr. Paulo Mota Pinto, *O Direito à Reserva...*, p. 526. No mesmo sentido, v. Teresa Alexandra Coelho Moreira, *Da Esfera Privada do Trabalhador...*, p. 106 e 107.

31 Cfr. Teresa Alexandra Coelho Moreira, *Da Esfera Privada do Trabalhador...,* p. 135.

32 V. a este respeito a reflexão de PAULO MOTA PINTO, quando refere a evolução jurisprudencial que ocorreu em torno do conteúdo desta definição, que praticamente reduziu o direito à reserva sobre a intimidade da vida privada ao controlo da informação sobre a vida privada, deixando de fora a liberdade da vida privada. (Cfr. Paulo Mota Pinto, *Direitos de Personalidade...*, p. 597-601)

Daqui resultam, desde logo, duas perspetivas que têm caraterizado o direito à reserva da vida privada: a possibilidade de conformação do direito pelo seu titular *(al. a)*; e a proibição de divulgação de aspetos que se inserem na reserva da vida privada, sem o consentimento do titular do direito *(al. b)*.

No que respeita à primeira perspetiva, é o próprio art. 80º do CC que determina que «a extensão da reserva é definida conforme a natureza do caso e a condição das pessoas», o que implica que sejam tidas em consideração as funções exercidas pelo trabalhador, o nível de autonomia e de confiança da relação laboral em questão, bem como a conformação que o titular do direito faz do seu conteúdo, estipulando o que considera estar protegido por esse direito e o que considera que já não faz parte do mesmo.

E esta primeira perspetiva assume grande relevo sobretudo porque estamos perante conceitos indeterminados, que carecem de uma concretização da parte do aplicador do Direito que, em função das caraterísticas de cada caso, terá que salvaguardar este direito das pessoas[33]. Essa concretização passa, desde logo, por identificar quais os aspetos que devem ser incluídos no conceito de reserva da vida privada e em que medida.

Foi precisamente com o objetivo de materializar o âmbito de proteção deste direito que, na doutrina alemã, se desenvolveu a teoria das três esferas[34], de acordo com a qual o direito à reserva da vida privada deveria ser decomposto em: esfera íntima ou de segredo (que engloba os factos que devem ser inacessíveis a terceiros, tais como aspetos da vida familiar e sexual, convicções religiosas e políticas, estado de saúde das pessoas); esfera privada (aspetos pessoais, aspetos relacionados com a residência ou com o trabalho, informação sobre hábitos diários e sobre animais de estimação, entre outros); e esfera pública (na qual se inserem as informações e os comportamentos que estão ao dispor de quem quiser).

Esta teoria foi igualmente defendida, entre nós, por Orlando De Carvalho[35] e dela parecem resultar diferentes níveis de proteção, consoante os aspetos se enquadrem na vida íntima ou na vida privada, sendo que as informações relativas à vida privada das pessoas teriam uma proteção menor do que as que respeitam à sua vida íntima.

Sucede que, como refere Mota Pinto, tal divisão poderia levar a que algumas situações que pertencem à chamada vida privada ficassem fora da proteção conferida pelo ordenamento jurídico, o que não se pretende[36].

---

33 Cfr. Diogo Figueiredo Perfeito Dias Ferreira, *Trabalhador, Reserva da Intimidade da Vida Privada e Redes Sociais: nótulas reflexivas sobre um delicado problema juslaboral,* [Cons. 18 mar. 2021] Disponível em <https://portal.oa.pt/media/132093/diogo-figueiredo-perfeito-dias-ferreira.pdf>, p. 589.

34 Vide por todos Paulo Mota Pinto, *O Direito à Reserva…,* nota 104.

35 Cfr. Orlando De Carvalho, *Teoria Geral do Direito Civil*, coord. Francisco Liberal Fernandes [et. al.], 3ª ed., Coimbra Editora, 2012, ISBN 978-972-32-2017-9, p. 265-266, nota 69.

36 Cfr. Paulo Mota Pinto, *O Direito à Reserva…*, p. 524-534.

Por sua vez, Menezes Cordeiro identifica, não três, mas cinco esferas de privacidade, com diferentes graus de proteção: esfera íntima, esfera secreta, esfera privada, esfera individual social e esfera pública[37]. Segundo este autor, as três primeiras esferas contêm informações que só podem ser acessíveis mediante o consentimento do seu titular, enquanto as duas últimas englobam informações que são parcial ou totalmente acessíveis.

Pese embora a divisão em esferas de privacidade auxilie na compreensão das diferenças existentes entre a multiplicidade de informações que cabem na reserva da vida privada das pessoas, bem como a sancionar de forma distinta violações que podem ter graus de censurabilidade diferentes, neste trabalho iremos considerar a reserva da vida privada em sentido amplo, sem distinguir entre as diferentes dimensões que a mesma pode assumir. Pelo que, quando nos reportamos ao direito à reserva da vida privada, consideramos que deve partir-se da premissa de que toda e qualquer ofensa à vida privada é proibida para depois, em casos concretos que o justifiquem, se permitirem exceções.

Aliás, parece ter sido este o entendimento seguido pelo legislador português, uma vez que nos diferentes diplomas onde podemos encontrar referências à reserva da vida privada, as normas começam por estabelecer a proibição de intromissão na vida privada das pessoas, prevendo depois exceções pontuais e justificadas por interesses superiores.

Portanto, podemos concluir que a primeira perspetiva enunciada se refere à conformação do direito à reserva da vida privada, que se encontra positivado de forma muito ampla, deixando ao seu titular a tarefa de definir o que se integra no seu núcleo mais íntimo, que só a ele diz respeito e que, por isso, merece especial tutela[38].

Já a segunda perspetiva refere-se ao direito à reserva da vida privada enquanto proteção da informação que o titular quer resguardar das outras pessoas, apenas chegando ao conhecimento daqueles que o titular autorizar a obter essas informações, mediante o seu consentimento que, sendo lícito, afasta a hipótese de violação do direito à reserva da vida privada. Esta perspetiva significa que o exercício do direito engloba afastar intromissões

---

37 Cfr. António Menezes Cordeiro, *Direito do Trabalho...*, p. 557-558.

38 Como refere MARIA REGINA REDINHA, «a latitude do conceito de reserva da vida privada não é abstratamente determinável, uma vez que varia de acordo com a particular posição do sujeito em causa, nomeadamente, notoriedade do sujeito, exposição pública, atividade profissional, funções desempenhadas, etc., e até com a própria circunscrição que o próprio traça para a sua privacidade, uma vez que a fronteira entre a esfera pública e privada é, em larga medida, definida pelo indivíduo» (Cfr. Maria Regina Gomes Redinha, *Direitos de personalidade - anotação aos artigos 16º a 21º do Código de Trabalho de 2003*, Trabalho Académico, Faculdade de Direito da Universidade do Porto, 2005, p. 2 [Cons. 17 mar. 2021] Disponível em <https://repositorio-aberto.up.pt/bitstream/10216/18694/2/39941.pdf>)

dos outros[39] (quer através da divulgação de aspetos da vida privada, quer através do mero acesso a essas informações). Tal evidencia uma caraterística do direito à reserva da vida privada, que é a possibilidade de autodeterminação informativa por parte do titular do direito[40].

Por outro lado, importa referir que o direito à reserva da vida privada goza de um poder de exigir comportamentos negativos e positivos, atribuindo ao legislador ordinário a tarefa de consagrar normas capazes de conferir proteção jurídica suficiente e adaptada às diversas vertentes que este direito pode assumir e, simultaneamente, determina a não intromissão de entidades públicas e privadas no núcleo mais íntimo da pessoa humana, a sua vida privada[41].

Além disso, distingue-se entre o direito à reserva da vida privada enquanto controlo da informação sobre a vida privada e o direito à liberdade da vida privada, sendo que este último se insere no direito ao livre desenvolvimento da personalidade.

Por fim, e no que respeita à titularidade do direito, importa referir que as empresas e outras pessoas coletivas também podem ser titulares do direito à reserva da vida privada, por força do art. 12º, nº 2 da CRP. Apesar disso, neste trabalho, referir-nos-emos apenas às pessoas singulares, na medida em que pretendemos uma análise da afetação deste direito na pessoa dos trabalhadores, que são sempre pessoas singulares[42].

2.4. FIGURAS AFINS

O direito à reserva da vida privada, pelo caráter lato que supra referimos, afigura-se de aplicação residual face a outros direitos de personalidade, tais como: o direito à inviolabilidade do domicílio, da correspondência e de outras

---

39 Neste sentido, GOMES CANOTILHO e VITAL MOREIRA, defendem que o direito à reserva da vida privada se analisa «em dois direitos menores: a) o direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar e b) o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem». (Cfr. J.J. Gomes Canotilho e Vital Moreira, *Constituição...*, p. 467 e 468)

40 Cfr. Paulo Mota Pinto, *Direitos de Personalidade...*, p. 605.

41 Como refere VIEIRA DE ANDRADE, «*As normas que prevêem os direitos, liberdades e garantias são normas preceptivas e conferem verdadeiros poderes de exigir de outrem (do Estado, pelo menos) um certo comportamento (geralmente a abstenção), ao mesmo tempo que impõem o dever correspondente. São direitos cujo conteúdo é constitucionalmente determinável e que não necessitam, por isso, para valerem como direitos, de intervenção legislativa.».* (Cfr. José Carlos Vieira De Andrade, *Os Direitos Fundamentais*..., p. 205)

42 Quanto a este tema, JOÃO LEAL AMADO refere que «o trabalhador é, necessariamente, uma pessoa singular», pois é isso mesmo que decorre do artigo 11º CT. (Cfr. João Leal Amado, C*ontrato de Trabalho: Noções Básicas,* 2ª ed., Almedina, 2018, ISBN 978-972-40-7438-2, p.47) Pelo contrário, MENEZES CORDEIRO defende que também as pessoas coletivas podem assumir na relação laboral a posição de trabalhadores, embora reconhecendo que algumas disposições do CT não lhe seriam aplicáveis. (Cfr. António Menezes Cordeiro, *Direito do Trabalho*..., p. 454-455)

comunicações; o direito à honra, reputação e bom nome; o direito à imagem; o direito à identidade pessoal; o direito de propriedade; entre outros.

Estes direitos tutelam uma vertente específica da personalidade, que pode ou não afetar a reserva da vida privada das pessoas, consoante o caso concreto, e são compatíveis com o direito à reserva da vida privada, podendo verificar-se uma violação do direito à reserva da vida privada em conjunto com a violação de um destes direitos[43].

Porém, é possível e frequente verificar-se uma ofensa a um destes direitos, sem que estejamos perante uma violação do direito à reserva da vida privada. Estes direitos podem inclusive ser violados fora da esfera privada, na esfera pública. Por isso, embora tenham elementos em comum, estes direitos de personalidade não se confundem com o direito à reserva da vida privada.

Outro direito que se relaciona frequentemente com a reserva da vida privada é o direito de autodeterminação informativa, que consta do art. 35º da CRP e que diz respeito à possibilidade de os cidadãos poderem gerir a utilização que é feita dos seus dados pessoais. Este direito distingue-se do direito à reserva da vida privada porque apenas diz respeito à utilização da informática e aos dados pessoais. Embora a utilização da informática possa gerar intrusões na vida privada, muitas vezes através do acesso e divulgação de dados pessoais, a verdade é que a reserva da vida privada vai muito para além disso, verificando-se, não raras vezes, intromissões na vida privada dos cidadãos sem estarem em causa dados pessoais e sem recurso aos meios informatizados.

Deste modo, ficam analisadas, ainda que de forma sucinta e numa perspetiva abstrata, as principais caraterísticas do direito à reserva da vida privada, bem como a especial tutela que lhe é conferida no seio dos direitos fundamentais, uma análise que nos permitirá compreender melhor a inserção deste direito na legislação laboral e as implicações práticas do mesmo na relação entre trabalhador e empregador, o que faremos de seguida.

3. RESERVA DA VIDA PRIVADA DOS TRABALHADORES

A prestação de trabalho evoluiu de tal forma nos últimos anos que se torna cada vez mais difícil traçar uma linha divisória entre o trabalho e a vida privada, quer porque o trabalho nos dias de hoje assume facetas muito variadas, podendo em certos casos ser prestado em casa do trabalhador[44]

[43] Sobre este tema v. Paulo Mota Pinto, *O Direito à Reserva…*, p. 539-552.

[44] Neste trabalho, referimo-nos ao trabalhador como «a pessoa que se encontra adstrita a desenvolver uma atividade, sob autoridade e a direção de outra», uma noção apontada por MENEZES CORDEIRO, que pressupõe a celebração de um contrato de trabalho, com as caraterísticas elencadas no artigo 12º CT. (Cfr. António Menezes Cordeiro, *Direito do Trabalho…,* p. 453.)

ou em qualquer outro lugar, onde se misturam aspetos da vida privada com o exercício das funções que competem ao trabalhador, quer porque existem horários que não permitem distinguir a jornada de trabalho dos restantes períodos do dia, quer ainda porque é no seio do trabalho, no contacto com os colegas ou na sede da empresa que o trabalhador desenvolve parte da sua personalidade, uma vez que é aí que passa grande parte da sua vida[45].

A relação laboral inicia-se com a celebração de um contrato de trabalho, um negócio jurídico bilateral, que pressupõe a prestação de uma atividade pelo trabalhador, mediante uma retribuição paga pelo empregador, atividade essa que é exercida de forma subordinada[46]. Ora, com a celebração do contrato, surgem direitos e obrigações para ambas as partes e o trabalhador vê a sua liberdade ser limitada, ficando sujeito ao poder diretivo (possibilidade de a entidade empregadora dar ordens ou instruções, bem como averiguar o cumprimento das regras e controlar a execução dos trabalhos), ao poder regulamentar (autonomia para estabelecer as regras de funcionamento da empresa e as formas de execução do trabalho) e ao poder disciplinar (faculdade de sancionar determinadas condutas dos trabalhadores) do empregador[47].

Portanto, conforme resulta do art. 11º do CT[48] e do art. 1152º do CC, ao celebrar o contrato de trabalho, o trabalhador obriga-se perante outrem e, por forma a dar cumprimento às obrigações assumidas, sofre uma restrição dos seus direitos de personalidade[49]. Todavia, mantém todos os seus direitos perante a entidade empregadora e perante os outros trabalhadores, continuando a reconhecer-se a cada pessoa a sua cidadania, independentemente da relação laboral em que se encontra[50].

A este respeito, Maria do Rosário Palma refere a existência de um princípio geral da preservação dos direitos de personalidade do trabalhador, enquanto cidadão, na pendência do contrato, que se desdobra em três projeções: a

---

45 Neste sentido, v. Frank Hendrickx, *Privacy, data protection and measuring employee performance. The triggers of technology and smart work*, European Labor Law Journal, 2018, vol. 9 (2), p. 99-100 [Cons. 17 mar. 2021] Disponível em <https://journals.sagepub.com/doi/full/10.1177/2031952518781448>.

46 Sobre os elementos caraterísticos do contrato de trabalho, v. Pedro Romano Martinez, *Direito do Trabalho*, 6ª ed., Almedina, 2013, ISBN 978-972-40-5146-8, p. 271-276.

47 Para mais desenvolvimentos sobre os poderes do empregador, v. Teresa Alexandra Coelho Moreira, *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo eletrónico do empregador*, Coimbra, Almedina, 2010, ISBN 978-972-40-4208-4, p. 343-379.

48 Com vista a uma análise atual da problemática em torno da reserva da vida privada, este trabalho tem como fonte a mais recente legislação de trabalho, designadamente a Lei n.º 7/2009, de 12 de Fevereiro.

49 Conforme refere MERCADER UGUINA, «a relação de trabalho é a única relação jurídica de caráter patrimonial que implica de modo direto a pessoa, a personalidade e mesmo a liberdade do trabalhador». (Cfr. Jesús R. Mercader Uguina, *Derecho del Trabajo: Nuevas tecnologías y sociedad de la información*, Valladolid , Editoral Lex Nova, 2002, p. 96)

50 Cfr. Maria Regina Redinha, *Direitos de personalidade…,* p. 1 e JOSÉ JOÃO ABRANTES, *Contrato de Trabalho...*, p. 59-63.

possibilidade de os trabalhadores exigirem ao empregador o respeito pelos seus direitos pessoais em qualquer fase do contrato; a sobreposição dos direitos de personalidade dos trabalhadores à autonomia privada e aos poderes do empregador; e o facto de, na relação laboral, os direitos de personalidade apenas poderem ser restringidos em situações excecionais, obedecendo ao princípio da proporcionalidade (art. 18º CRP) e com respeito pelos limites impostos pela ordem pública (art. 81º do CC)[51].

No que respeita aos direitos fundamentais dos trabalhadores, podemos distinguir entre direitos fundamentais específicos e direitos fundamentais inespecíficos[52]. Os primeiros referem-se aos direitos consagrados na Constituição, mas que apenas são reconhecidos como direitos de um determinado cidadão quando este assume a qualidade de trabalhador, ou seja, são direitos que apenas ganham efetividade na relação laboral. Já os direitos fundamentais inespecíficos são os direitos que a Constituição reconhece a todos os cidadãos, pelo simples facto de o serem[53]. A reserva da vida privada é um direito fundamental inespecífico que, sendo inerente a todas as pessoas, assume algumas particularidades no contexto de trabalho.

Assim, na relação laboral, os trabalhadores mantêm os seus direitos fundamentais e os seus direitos de personalidade, entre os quais o direito à reserva da vida privada. Aliás, são eles que vão limitar o exercício dos poderes do empregador, salvaguardando a dignidade dos trabalhadores que, como refere Monero Pérez[54], é uma projeção do princípio fundamental da dignidade da pessoa humana.

3.1. A EVOLUÇÃO DO CÓDIGO DO TRABALHO

A evolução do Código do Trabalho demonstra a preocupação do legislador compatibilizar a promoção da igualdade e a defesa dos direitos de personalidade do trabalhador com a liberdade de gestão empresarial e o exercício de poderes pelo empregador.

Não obstante o exercício de poderes por parte da entidade empregadora ser essencial na relação laboral, tem vindo a registar-se um aumento do poder de controlo em virtude da introdução das novas tecnologias nas empresas, sendo que a utilização das mesmas implica frequentemente uma

---

51 Cfr. Maria Do Rosário Palma Ramalho, *Tutela da personalidade e equilíbrio entre interesses dos trabalhadores e dos empregadores no contrato de trabalho. Breves Notas*, p. 4 [Cons. 18 mar. 2021] Disponível em:<https://www.stj.pt/wp-content/uploads/2014/10/prof_maria_rosario_ramalho.pdf>.

52 Cfr. António Monteiro Fernandes, *Direito do Trabalho*, 19ª ed., Almedina, 2019, ISBN 978-972-40-8076-5, p. 277-279.

53 A este respeito, v. Teresa Alexandra Coelho Moreira, *Da Esfera Privada do Trabalhador…*, p.41-43.

54 Cfr. José Luís Monereo Pérez, *La dignidad del trabajador, Dignidad de la persona en el sistema de relaciones laborales*, Murcia, Ediciones Laborum S.L., 2019, ISBN 978-84-17789-25-1, p. 161.

intrusão na vida privada dos trabalhadores. Por esse motivo, o uso destes meios no contexto laboral deve ser regulamentado, evitando que a celebração de um contrato de trabalho signifique para o trabalhador a supressão dos seus direitos de personalidade.

Foi neste sentido que o CT de 2003 dedicou, pela primeira vez na legislação laboral portuguesa, um conjunto de normas aos direitos de personalidade do trabalhador. Pese embora o caráter de direitos de personalidade fosse suficiente para os tornar efetivos na relação laboral, o legislador optou por transpor os direitos de personalidade consagrados na CRP e no CC para o CT, aprofundando alguns pontos mais controversos e mantendo outros com alguma margem de discricionariedade[55], sem prejuízo de as normas integradas nesses diplomas continuarem a ser aplicáveis na relação laboral.

Conforme refere Guilherme Dray[56], tal posicionamento do legislador não foi desprovido de sentido, mas antes parece assentar em quatro razões fundamentais.

Em primeiro lugar, o legislador reconheceu que os direitos de personalidade regulados no CC estão pensados para as relações entre partes iguais (relações horizontais), pelo que fazia todo o sentido autonomizar estes direitos e consagrá-los na legislação laboral, onde as partes contratuais estão longe de se encontrarem em posições paritárias, uma vez que uma entidade exerce poder sobre a outra (relações verticais).

Em segundo lugar, existem questões específicas que são suscitadas na relação laboral e que, por todo o contexto que subjaz à mesma, justificam uma atenção e regulação especial.

Em terceiro lugar, ao celebrar um contrato de trabalho, o trabalhador assume colocar a sua força de trabalho, o seu conhecimento e, verdadeiramente, a sua pessoa, ao serviço do trabalho que se compromete desempenhar, o que implica uma afetação dos seus direitos.

Por último, os avanços tecnológicos e os meios de comunicação colocados à disposição do empregador e usados, muitas vezes, como instrumentos de trabalho, permitem novas formas de intromissão na esfera privada, sobretudo através de dispositivos que têm em vista o exercício do poder de controlo do empregador sobre os trabalhadores.

Nesse sentido, o CT de 2009 veio prever expressamente a liberdade de expressão e de opinião, a integridade física e moral, a reserva da intimidade da vida privada, a proteção de dados pessoais e dos dados biométricos, o recurso a testes e exames médicos, a limitação dos meios de vigilância à distância e a confidencialidade de mensagens e de acesso à informação. Esses direitos encontram-se nos artigos 14º e ss, sob a epígrafe "*direitos de personalidade*".

---

55 Cfr. Pedro Romano Martinez, *Direito do Trabalho…*, p. 340-343.

56 Cfr. Guilherme Dray, *An Introduction to Portuguese Employment & Labour Law*, colab. Catarina Granadeiro, Coimbra, Almedina, 2019, ISBN 978-972-40-8108-3, p. 53.

A reserva da intimidade da vida privada está prevista no art. 16º do CT, cujo nº 1 determina que quer o empregador quer o trabalhador devem obediência aos direitos de personalidade da contraparte, uma opção legislativa difícil de compreender uma vez que, como Regina Redinha[57], consideramos que o empregador não necessitava desta proteção especial que a lei lhe confere. Pese embora seja parte no mesmo contrato que o trabalhador, o empregador detém, mesmo antes da celebração do contrato, uma posição de superioridade económica e jurídica, que não diminui com a celebração desse contrato. Aliás, em nenhum momento o contrato de trabalho limita os direitos do empregador. Pelo contrário, os trabalhadores veem a sua pessoa implicada com a celebração do contrato, na medida em que têm que aceitar determinadas restrições ao exercício dos seus direitos e, consequentemente, ao livre desenvolvimento da sua personalidade. Portanto, perante esta desigualdade das partes, que torna os trabalhadores os contraentes mais débeis, entendemos que o legislador deveria ter-se preocupado em acautelar os interesses daqueles que efetivamente precisam de proteção. Ao invés, adotou uma formulação paritária, tratando de forma igual pessoas jurídicas que detém, desde a celebração até à cessão do contrato, posições desiguais[58].

Por seu turno, o nº 2 desse artigo dispõe que este direito «*abrange quer o acesso, quer a divulgação de aspectos atinentes à esfera íntima e pessoal das partes, nomeadamente relacionados com a vida familiar, afectiva e sexual, com o estado de saúde e com as convicções políticas e religiosas*», procurando com isso enunciar alguns aspetos que integram a intimidade da vida privada, embora não de forma taxativa. Assim, o art. 16º, nº2 do CT abrange toda e qualquer intromissão de terceiros na vida privada dos trabalhadores, independentemente de a forma de obtenção das informações ser ou não lícita.

Segue-se o art. 17º, que proíbe o empregador de exigir aos candidatos a emprego ou aos seus trabalhadores informações relativas à sua vida privada, à sua saúde ou estado de gravidez, salvo se alguma destas informações for necessária para avaliar a aptidão para o trabalho, devendo nesse caso a fundamentação ser fornecida por escrito. Este artigo vem concretizar na relação laboral a proteção de dados pessoais estabelecida no art. 35º da CRP e na Lei nº 58/2019, de 08-08-2019, reforçando a conexão entre dados pessoais e vida privada. E, ao contrário da norma anterior, dirige-se apenas os trabalhadores ou candidatos a emprego. Além disso, a proteção prevista destina-se à recolha de informações sobre a vida privada dos trabalhadores, estipulando a possibilidade de a entidade empregadora solicitar tais infor-

---

57 Cfr. Maria Regina Gomes Redinha, *Direitos de personalidade…,* p. 1.

58 No mesmo sentido, MONTEIRO FERNANDES, refere que *«trata-se de uma paridade mistificatória, uma vez que o empregador só em medida muito limitada, ou mesmo nula, implica a sua pessoa na relação de trabalho.».* (Cfr. António Monteiro Fernandes, *Direito do Trabalho...,* nota 23) Por sua vez, Maria Do Rosário Palma Ramalho defende que esta opção legislativa não passa de uma perspetiva formal. (Cfr. Maria Do Rosário Palma Ramalho, *Tutela da personalidade…,* p. 6)

mações quando existir um interesse subjacente à relação laboral que torne o seu conhecimento necessário, salvo situações excecionais que não permitem o acesso de modo algum[59].

O art. 19º do CT refere-se aos testes e exames médicos, dispondo que o empregador não pode, em princípio, exigir ao candidato a emprego ou ao trabalhador a realização ou apresentação de testes ou exames médicos, salvo se estes tiverem em vista a proteção e segurança do trabalhador ou de terceiros, ou se particulares exigências inerentes à atividade o justificarem. Este preceito está diretamente relacionado com a saúde dos trabalhadores e candidatos a emprego, pelo que integra a vida privada dos mesmos.

Importa ainda referir a introdução do art. 20º do CT relativo à utilização de meios de vigilância à distância, uma vez que estes podem captar aspetos da vida privada dos trabalhadores. Assim, o nº 1 deste artigo afirma ser proibida a utilização destes mecanismos para controlar os trabalhadores, pelo que os mesmos apenas são admitidos se existir um motivo legítimo, tal como assegurar a segurança do local de trabalho, com o objetivo de proteger pessoas e/ou bens, e desde que se comprove o risco de violação dessa segurança.

Por fim, o art. 22º estabelece a confidencialidade de mensagens e informação de caráter não profissional «consultada pelo trabalhador no tempo e local de trabalho através da utilização de meios ou instrumentos de trabalho, colocados à sua disposição pelo empregador», o que se tornou mais frequente com a utilização dos computadores e do correio eletrónico, e tem correspondência no art. 34º da CRP.

Todos estes preceitos foram inovadores, pois nenhum deles encontra correspondência nas versões anteriores do CT de 2009 ou da restante legislação laboral. E todos eles têm em comum o bem jurídico protegido: a inviolabilidade pessoal dos trabalhadores, sendo habitualmente considerados projeções do direito à reserva da vida privada.

Além disso, os preceitos consagrados no CT permitem-nos concluir que existiu uma preocupação do legislador conferir proteção a este direito, adotando como regra «o princípio da irrelevância das matérias da esfera privada das partes para o contrato de trabalho»[60]. Contudo, parece-nos que o legislador português ficou ainda aquém das expectativas pois, nos dias que correm, com as inúmeras ameaças que existem e que são já reconhecidas pela doutrina e pela jurisprudência, direitos como a reserva da vida privada carecem não só de uma proteção abstrata, mas também de normas de efetivação.

Nesse sentido, consideramos que, mais do que respeitar o direito à reserva da vida privada dos trabalhadores, os empregadores deveriam ser responsáveis por garantir esse mesmo direito, o que não só iria balizar a sua própria atuação como permitiria uma atuação mais eficaz na prevenção de violações deste direito por parte dos trabalhadores entre si.

---

59 Cfr. António Monteiro Fernandes, *Direito do Trabalho...,* p. 291.

60 Cfr. Maria Do Rosário Palma Ramalho, *Tutela da personalidade…*, p. 7.

Assim, e sem descurar a evolução legislativa inovadora que se verificou em Portugal relativamente a esta matéria, somos de opinião que ainda existem muitos espaços de discricionariedade que podem ser regulamentados, de modo a evitar abusos de poder pois, como Guy Davidov[61], acreditamos que a legislação laboral é um importante instrumento de justiça social, que permite atenuar a desigualdade entre trabalhadores e empregadores.

3.2. RELAÇÃO DESIGUAL: DA CONTRATAÇÃO À EXECUÇÃO DO CONTRATO

Pese embora estejamos perante uma relação entre dois sujeitos de direito privado, a mesma é profundamente afetada pelo sinalagma trabalho-salário, que provoca desigualdade entre as partes, não só a nível económico, mas, sobretudo, a nível da formação da vontade[62].

O trabalhador, em regra, carece dos rendimentos do trabalho para fazer face às suas despesas mais básicas (dependência económica), pelo que estará mais predisposto a aceitar as condições apresentadas pelo empregador, com o objetivo de ser escolhido para a vaga a que se candidata ou de manter o lugar que detém no seio da empresa, consoante a fase contratual em que se encontre. Pelo contrário, o empregador poderá encontrar outras pessoas disponíveis para desempenhar as mesmas funções, com as mesmas ou semelhantes habilitações e que estejam dispostas a ceder perante aquilo que lhe for proposto.

Além disso, existe uma maior afetação da pessoa do trabalhador na relação de trabalho do que do empregador, o que leva muitos autores a referir-se ao contrato de trabalho como sendo um contrato *intuitu personae*[63].

Acresce que, durante a execução do contrato, o trabalhador fica sujeito aos poderes de direção e controlo do empregador (subordinação jurídica)[64], levando a que a desigualdade entre as partes que se verifica no momento da contratação, se mantenha após a mesma.

Obviamente que, como refere José João Abrantes[65], «a relação de trabalho não é sempre uma relação desigual favorável ao empregador: a situação pode muitas vezes aparecer invertida» em virtude das mais variadas circunstâncias pessoais, familiares, económicas e até relacionadas com o tipo de trabalho e com a profissão em causa. Contudo, a tendência é a da exis-

---

61 Cfr. Guy Davidov, *The Enforcement Crisis in Labour Law and the Fallacy of Voluntarist Solutions*, The International Journal of Comparative Labor Law and Industrial Relations 26, no. 1, Kluwer Law International BV, The Netherlands, 2010, p. 61-81, ISSN 0952-617X [Cons. 17 mar. 2021] Disponível em <https://www.academia.edu/17924292/The_Enforcement_Crisis_in_Labour_Law_And_the_Fallacy_of_Voluntarist_Solutions>, p. 80. No mesmo sentido, Teresa Alexandra Coelho Moreira, *A Privacidade dos Trabalhadores...*, p. 346.

62 Cfr. José João Nunes Abrantes, *Contrato de Trabalho…*, p. 44-50.

63 Cfr. Teresa Alexandra Coelho Moreira, *A Privacidade dos Trabalhadores…,* p. 337.

64 Cfr. João Leal Amado, *Contrato de Trabalho...*, p. 13.

65 Cfr. José João Nunes Abrantes, *Contrato de Trabalho…*, nota 3.

tência de uma desigualdade das partes marcada pela dependência económica e jurídica do trabalhador face ao empregador[66].

Além disso, verifica-se que quanto maior a desigualdade económica e social entre o empregador e o trabalhador, mais acentuado é o constrangimento deste último, que se sente muitas vezes forçado a concordar com as cláusulas contratuais que lhe são apresentadas, a autorizar o acesso aos seus dados pessoais e a divulgar aspetos da sua vida privada, que preferia manter para si ou partilhar com um círculo restrito de pessoas.

Perante esta factualidade, claro se torna que, no momento da contratação, quando ainda não possui o vínculo contratual que lhe atribuirá o seu sustento, a posição do candidato a emprego é ainda mais frágil do que aquela que poderá vir a assumir enquanto trabalhador[67], em virtude da sua dependência económica e da conjuntura de emprego existente.

E se, por um lado, é legítimo a entidade empregadora tomar conhecimento de algumas informações da vida privada das pessoas, que podem ser relevantes para aferir a idoneidade do candidato para o cargo que se propõe assumir e, consequentemente para a decisão de contratar, o certo é que, com base nessas informações, pode haver discriminação entre candidatos com fundamento em determinadas informações que os mesmos se viram obrigados a prestar e que, muitas vezes, determinam a sua exclusão do processo de recrutamento, mesmo que nada tenham que ver com a execução do trabalho[68]. Isto verifica-se porque não existe um critério para averiguar quais as informações necessárias para aferir da aptidão para o trabalho, cabendo ao empregador definir as perguntas que faz, como faz e o que faz com as respostas.

Já na fase de execução do contrato, a desigualdade entre as partes sente-se sobretudo quanto à liberdade de atuação e à insegurança na manutenção do vínculo laboral. Enquanto a entidade patronal dispõe de grande liberdade para a conformação dos moldes de execução do contrato, os trabalhadores veem a sua liberdade ser restringida durante o tempo de trabalho em função das regras que lhes são impostas pelo empregador e às quais devem obediência.

---

66 Foi precisamente com base na necessidade de proteger os trabalhadores enquanto sujeitos contratuais mais frágeis que surgiu, no século XIX, o Direito do Trabalho, como ramo autónomo do direito civil. Cfr. Teresa Alexandra Coelho Moreira, *A Privacidade dos Trabalhadores...*, p. 347.

67 V. a este respeito Teresa Alexandra Coelho Moreira, *Da Esfera Privada do Trabalhador...*, p. 148.

68 Assim, concordamos plenamente com TERESA MOREIRA, quando afirma que «o interesse legítimo do empregador em obter dados sobre a idoneidade e aptidão do candidato para o posto de trabalho encontra-se limitado pelo respeito devido aos direitos fundamentais do trabalhador de não suportar ingerências injustificadas na sua esfera privada e de não ser discriminado por caraterísticas pessoais.» (Cfr. Teresa Alexandra Coelho Moreira, *Da Esfera Privada do Trabalhador…*, p. 212)

Ademais, o empregador não tem uma preocupação tão grande com a manutenção dos contratos de trabalho como os próprios trabalhadores, uma vez que ao contrário destes últimos que, se perderem o emprego, poderão deparar-se com grandes dificuldades em encontrar outro que se adeque às suas necessidades e expectativas, o empregador não depende desses contratos, podendo admitir novos trabalhadores num curto espaço de tempo[69].

3.3. DEVER DE INFORMAÇÃO

Conforme vimos no título anterior, o trabalhador é questionado pela entidade empregadora acerca de uma série de informações que podem estar relacionadas com a execução do contrato, direta ou indiretamente. Contudo, o que se verifica muitas vezes é que, entre as informações solicitadas, algumas são lícitas e outras não, o que está relacionado com o dever de informação que recai sobre ambas as partes na relação laboral.

O art. 106º do CT, sob a epígrafe *"Dever de Informação"*, estabelece no seu nº 1 a obrigatoriedade de o empregador informar o candidato a trabalhador sobre os aspetos relevantes do contrato de trabalho, de que são exemplo as informações elencadas no nº3 do mesmo artigo.

A este respeito, importa referir que a Diretiva (UE) 2019/1152, de 20 de junho de 2019, relativa a condições de trabalho transparentes e previsíveis na União Europeia veio alargar o dever de informação que impende sobre a entidade empregadora, no sentido de conferir a todos os trabalhadores «um grau adequado de transparência e previsibilidade»[70]. Além de acentuar o dever de informação que recai sobre o empregador, a Diretiva em questão estipula que o empregador tem que prestar ao trabalhador ou candidato a emprego inúmeras informações que habitualmente se abstinha de comunicar, designadamente sobre o direito a formação, sobre os prazos para impugnação do despedimento e sobre os detalhes da remuneração. Ademais, o requisito de todas as informações serem prestadas por escrito, consignado no art. 3º da Diretiva, bem como as sanções previstas para os empregadores que não respeitarem tal imposição legal, garantem mais confiança e segurança aos trabalhadores.

Por sua vez, o nº 2 do art. 106º do CT determina a obrigatoriedade de o trabalhador ou candidato a emprego *«informar o empregador sobre aspetos relevantes para a prestação da atividade laboral»,* deixando de fora todas as

---

69 Neste sentido v. António Menezes Cordeiro, *Direito do Trabalho…*, p. 433.

70 Cfr. DIRETIVA (UE) 2019/1152 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa a condições de trabalho transparentes e previsíveis na UE, ponto 6 do preâmbulo [Cons. 27 mai. 2021] Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32019L1152>. A transposição da referida Diretiva para o ordenamento jurídico português está prevista na Proposta de Lei n.º 15/XV/1, que prevê uma alteração de legislação laboral no âmbito da agenda de trabalho digno.

questões da vida privada que não tenham que ver diretamente com a execução do trabalho para o qual é contratado.

Apesar de ser esta a letra da lei e de o mesmo entendimento ser unânime na doutrina e na jurisprudência, a verdade é que, constantemente, a entidade empregadora questiona os trabalhadores e os candidatos a emprego sobre aspetos que vão para além do necessário para a sua contratação e que implicam uma intromissão na vida privada daqueles.

Nessas situações, o dever de informação não poderá ser aplicado tal e qual como está previsto na lei, devendo antes o trabalhador ou candidato a emprego ter direito a não responder às questões colocadas, ou até mesmo a responder com informações falsas, de modo a salvaguardar a sua esfera privada, já que o dever de obediência que impende sobre si e que está previsto no art. 121º, nº 1, *al. d)* do CT funciona em sentido inverso, conferindo-lhe «*um verdadeiro direito de desobediência e de resistência face a ordens ilegítimas ou ilegais*»[71].

Pese embora, à luz do princípio da atuação da boa-fé, previsto no art. 126º do CT, esta possibilidade de mentir à entidade empregadora possa parecer contraditória, não o é, pois *«a boa fé não manda responder com verdade a quem coloca questões ilegítimas e impertinentes»*.[72] Ademais, o princípio da boa fé na execução do contrato impõe-se a ambas as partes, pelo que o empregador, ao fazer determinadas perguntas, não o estará a respeitar.

Acresce que, apesar de a vulnerabilidade do candidato a emprego ser, em princípio, superior à do trabalhador, a verdade é que mesmo durante a execução do contrato continuam a verificar-se situações deste género que atentam contra a reserva da vida privada dos trabalhadores. Além do mais, a desigualdade de poderes entre as partes contratuais, a subordinação jurídica e a dependência económica dos trabalhadores, regra geral, mantêm-se durante a relação laboral, o que justifica que, mesmo quando o trabalhador já possui um vínculo laboral com a entidade empregadora, continue a beneficiar desta possibilidade de reação.

Os principais motivos que legitimam esta ocultação da verdade ou, em *ultima ratio,* a mentira, da parte do trabalhador ou candidato a emprego são a posição frágil em que se encontra e que poderá ser acentuada se o empregador recusar contratá-lo ou decidir despedi-lo com base em informações que, à priori, nem deveria ter conhecimento, bem como um abuso de poder por parte do empregador que pretende saber mais do que o necessário.

O que sucede é que, enquanto o trabalhador pretende resguardar as informações da sua vida privada, a entidade empregadora quer escrutinar ao máximo essas informações, que podem ter algum tipo de influência na exe-

---

71 Cfr. Teresa Alexandra Coelho Moreira, *Da Esfera Privada do Trabalhador...,* p. 248.

72 Cfr. João Leal Amado, *Contrato de Trabalho...*, p. 146 e 147.

cução do contrato de trabalho[73]. Portanto, verifica-se um conflito entre o direito à reserva da vida privada do trabalhador e o direito de informação do empregador, cuja resolução passa por sobrepor o direito do trabalhador ao direito do empregador, nos termos do art. 335º do CC[74].

Ora, se para o empregador não existe propriamente um escrutínio dos motivos que levam a contratar determinado trabalhador em detrimento de outro, sem prejuízo do disposto no art. 25º do CT quanto à proibição de discriminação, parece-nos legítimo que o trabalhador, que só por si já detêm um poder negocial menor sobre os termos da relação de trabalho, possua algum meio de defesa face a uma tentativa de intromissão na sua esfera privada, como a possibilidade de ocultar ou mentir sobre determinadas questões relativas à sua vida privada, sendo certo que, em muitos casos, e conforme refere João Leal Amado[75], a mentira poderá ser a única forma de garantir o direito à reserva da vida privada dos trabalhadores ou candidatos a emprego que, de outra forma, poderiam sofrer tratamentos discriminatórios ou represálias.

Quando muito, esta conduta levada a cabo pelos trabalhadores poderá consubstanciar uma desobediência legítima, nos termos dos artigos 128º, nº 1, *al. e)* e 351º, nº 2, *al. a)* do CT, bem como do art. 21º da CRP[76]. Pelo contrário, a mentira em resposta a uma pergunta legítima será, de acordo com a doutrina, suscetível de sujeitar o trabalhador a responsabilidade civil pré-contratual, determinar a invalidade do contrato ou até justificar um despedimento.

3.4. CONFLITO DE INTERESSES

Desde os seus primórdios que o direito do trabalho sempre teve em consideração os diferentes interesses perspetivados pelos sujeitos contratuais, procurando compatibilizá-los.

De um modo geral, a entidade empregadora prossegue o lucro, a maior produtividade ao menor preço e tende a considerar necessário obter o máximo de informações possível sobre os seus trabalhadores ou candidatos a emprego, de forma a melhor discernir sobre a personalidade daqueles e sobre a sua aptidão para o trabalho. Pelo contrário, as principais preocupações dos trabalhadores são quase sempre ter boas condições de trabalho, salários apelativos e algumas regalias que lhes permitam fazer face aos encargos da sua vida e, simultaneamente, sentir-se bem no local e no tempo de trabalho.

---

73 Cfr. Francisco Javier Calvo Gallego, *Reputación digital y efectos sobre los trabajadores: redes sociales para contratación, usos y límites*, in Vigilancia y Control en el Derecho Trabajo Digital, Thomson Reuters, Aranzadi, 2020, ISBN 978-84-1346-553-1, p. 427 e 428.

74 Cfr. Maria Do Rosário Palma Ramalho, *Tutela da personalidade...*, p. 8.

75 Cfr. João Leal Amado, *Contrato de trabalho e "direito à mentira": uma solução justa?*, in Revista de Legislação e Jurisprudência, Ano 150º, Nº 4028, Gestelegal, Mai/Jun 2021, ISSN 0870-8487, p. 257-264.

76 Cfr. Teresa Alexandra Coelho Moreira, *A Privacidade dos Trabalhadores…*, p. 360-362.

Com os desenvolvimentos tecnológicos e a evolução da legislação laboral, essa dualidade de interesses não deixou de existir, mas adaptou-se aos tempos hodiernos. Assim, depois de se alcançarem as principais conquistas ao nível da proteção dos direitos dos trabalhadores na relação laboral, o direito do trabalho começou a atender também aos objetivos empresariais, procurando um equilíbrio entre os interesses de ambas as partes.

Pese embora se reconheça que estamos perante interesses conflituantes[77], na maior parte dos casos, não é possível abdicar totalmente de um deles, nem é aceitável estabelecer uma hierarquia de direitos, pelo que a solução passará sempre por uma compatibilização, isto é um equilíbrio assente no critério da proporcionalidade[78]. Por esse motivo, aquilo que hoje se exige ao legislador laboral e ao aplicador do direito é precisamente a compatibilização entre interesses que conflituam, de modo a não sacrificar exageradamente um em detrimento do outro[79].

Este raciocínio transposto para a problemática que é objeto deste estudo significa que o direito à reserva da vida privada dos trabalhadores e os interesses do empregador podem, de facto, ser interesses contrapostos, mas existe margem para os compatibilizar. Para tal, importa desde logo perceber quais os motivos que se encontram na origem do conflito.

Um dos motivos que leva a que os trabalhadores procurem resguardar os aspetos da sua vida privada na relação laboral é o facto de considerarem que essas informações não são relevantes para o desempenho do seu trabalho, bem como o receio de que o conhecimento dessas informações pela entidade empregadora possa gerar comportamentos discriminatórios em relação a si. Pelo contrário, o empregador considera tais informações de extrema importância para ter um conhecimento mais amplo do estilo de vida dos seus trabalhadores e assim saber o que esperar da conduta de cada um[80].

---

77 Quanto a este tema, v. Guilherme Dray, *An Introduction to...*, p. 18 e 19 e ainda João Leal Amado, *Contrato de Trabalho…* p. 187-191.

78 Neste sentido, v. José Vieira De Andrade, *Os Direitos Fundamentais...,* p.220-223.

79 Isso mesmo decorre do Ac. do TC nº 413/2011, onde se pode ler que «Sempre que um direito conflitue com outro direito ou bens constitucionalmente protegidos, esse conflito deve ser resolvido através da recíproca e proporcional limitação de ambos, em ordem a optimizar a solução (princípio da concordância prática) de modo a garantir uma relação de convivência equilibrada e harmónica em toda a medida possível.» (Cfr. Ac. do TC nº 413/2011, de 03.11.2011, Processo nº 20/11 [Cons. 29 mai. 2021] Disponível em: <https://dre.pt/web/guest/pesquisa-avancada/-/asearch/3280870/details/normal?emissor=Tribunal+Constitucional&perPage=100&types=JURISPRUDENCIA&search=Pesquisar>.

80 Neste contexto, MOTA PINTO refere que na relação laboral temos «de um lado, o interesse do indivíduo na sua privacidade, isto é, em subtrair-se à atenção dos outros, em impedir o acesso a si próprio ou em obstar à tomada de conhecimento ou à divulgação de informação pessoal (...); de outro lado, fundamentalmente, o interesse em conhecer e em divulgar informação conhecida, além do mais raro interesse em ter acesso ou controlar os movimentos do indivíduo». (Cfr. Paulo Mota Pinto, *O Direito à Reserva…*, p. 508-509)

Outro motivo que leva os trabalhadores a quererem manter em segredo aspetos da vida privada são os constrangimentos que podem sentir caso, no seu local de trabalho, essas informações se tornem conhecidas, quer perante o empregador, quer perante os colegas. Por seu turno, os empregadores invocam como fundamentos para acederem a informações da vida privada razões de eficiência, o exercício do seu poder de controlo, o direito de propriedade sobre os instrumentos de trabalho colocados à disposição dos trabalhadores, entre outros[81].

Sucede que, o princípio da liberdade de empresa fundamenta os poderes de direção e fiscalização, bem como a possibilidade de controlo exercida pelo empregador[82]. Pelo que, a entidade empregadora tende a justificar o controlo exercido através dos meios de comunicação e de vigilância com uma finalidade preventiva (averiguar se os trabalhadores estão a fazer um bom uso dos instrumentos de trabalho e a executar corretamente as suas funções) e com uma finalidade reativa (comprovar um incumprimento que se suspeita ou detetou e aplicar a respetiva sanção)[83]. Posto isto, torna-se necessário encontrar um equilíbrio entre o direito à reserva da vida privada dos trabalhadores e os direitos e interesses do empregador.

Sendo certo que os direitos de personalidade, entre os quais o direito à reserva da vida privada, podem ser objeto de restrições com fundamento na necessária harmonização com as regras do direito privado, não pode deixar de se atender a que essas restrições apenas poderão ocorrer se superarem o teste da proporcionalidade e se comprovar que não colocam em causa o próprio direito, pois nem o poder de direção do empregador, nem a subordinação jurídica do trabalhador podem resultar numa limitação excessiva ou arbitrária dos direitos de personalidade reconhecidos aos trabalhadores, na relação laboral e fora dela[84]. Por esse motivo, informações que digam respeito à vida privada dos trabalhadores e que cheguem ao conhecimento da entidade empregadora, seja por que motivo for, lícito ou ilícito, não podem, em princípio, servir de base para uma sanção.

Desta compatibilização de interesses resulta que apenas será de admitir uma intrusão na vida privada dos trabalhadores se a mesma tiver como fundamento um interesse legítimo da entidade empregadora. Aliás, a Convenção nº 111 da Organização Internacional do Trabalho[85] já dispunha que a enti-

---

81 Cfr. Jeremy De Beer, *Employee Privacy: The Need for Comprehensive Protection*, in Saskatchewan Law Review, vol. 66 (2), 2003, 388-390 [Cons. 17 mar. 2021] Disponível em: <https://www.academia.edu/15579733/Employee_Privacy_The_Need_for_Comprehensive_Protection>.

82 Cfr. Manuel Luque Parra e Francisco Ramón Lacomba, *Acceso a dispositivos digitales del trabajador*, in Vigilancia y control..., p. 357.

83 Cfr. Manuel Luque Parra e Francisco Ramón Lacomba, *Acceso a dispositivos digitales del trabajador*, in Vigilancia y control..., p. 357.

84 Cfr. José João Nunes Abrantes, *Contrato de Trabalho…*, p. 42 e 174.

85 Ratificada por Portugal através do DL nº 42/520, de 23 de setembro de 1959.

dade empregadora apenas pode aceder e tratar de «informações pessoais necessárias e imprescindíveis para a execução da prestação laboral», devendo ser essa a ideia subjacente a toda e qualquer compatibilização de interesses que opere neste âmbito.

3.5. VIOLAÇÃO DO DIREITO

Não obstante o reconhecimento do direito à reserva da vida privada por parte das entidades empregadoras, o conflito de interesses existente entre estas e os seus trabalhadores leva a que, por vezes, se verifique uma violação desse direito no contexto laboral. Tal violação pode resultar de um ato intencional da entidade empregadora ou, pelo contrário, pode ocorrer involuntariamente. Assim, na execução do contrato de trabalho, são inúmeras as possibilidades de violação do direito à reserva da vida privada e os contornos que a mesma pode assumir.

A título de exemplo, enunciaremos de seguida algumas situações suscetíveis de constituir uma violação deste direito, com o objetivo de demonstrar a linha ténue que existe entre o exercício legítimo de poderes do empregador e a violação do direito à reserva da vida privada dos trabalhadores.

Uma das formas de violação do direito à reserva da vida privada dos trabalhadores prende-se com as perguntas e questionários elaborados pela entidade empregadora, a fim de obter informações relativas aos seus trabalhadores. Nesses casos, a violação verifica-se quando a entidade empregadora ultrapassa os limites da necessidade e adequação nas perguntas efetuadas, questionando os trabalhadores sobre informações irrelevantes para o trabalho.

Da mesma forma, verifica-se uma violação do direito à reserva da vida privada quando os empregadores impõem aos seus trabalhadores a realização de testes para controlo do uso de estupefacientes ou da ingerência de álcool, bem como a realização de testes genéticos, psicológicos ou outros, sem apresentarem um motivo legítimo para o efeito.

Paralelamente, podemos falar de uma violação do direito quando a entidade empregadora abre ou lê correspondência dos seus trabalhadores, seja em formato físico (cartas; documentos) ou em formato digital (e-mails; mensagens). A este respeito, importa referir que, em princípio, apenas haverá violação do direito se o meio de comunicação utilizado permitir ao trabalhador uma expectativa razoável de privacidade. Pelo contrário, se o trabalhador utilizar meios de comunicação da empresa, como por exemplo uma conta de correio eletrónico coletivo, parece razoável admitir o acesso do empregador às mensagens, visto que a expectativa de privacidade é reduzida[86]. Além disso, o acesso do empregador à correspondência poderá não

[86] Cfr. Maria Regina Redinha; Maria Raquel Guimarães, *O uso do correio eletrónico no local de trabalho - Algumas reflexões*, in *Estudos em homenagem ao Professor Doutor*

constituir uma violação do direito se se verificar uma situação de abuso, que justifique o controlo dos meios utilizados[87], com a finalidade de a entidade empregadora compreender a dimensão da conduta do trabalhador, corrigir a situação e aplicar a devida sanção.

Outra forma de a entidade empregadora atentar contra o direito à reserva da vida ocorre com a monotorização eletrónica que opera nos instrumentos de trabalho em inúmeras empresas e que pode ocorrer através de sistemas de gravação de imagem e voz; softwares que controlam os movimentos dos trabalhadores no computador e nas instalações da empresa; dispositivos que localizam os veículos utilizados no horário laboral; programas que registam as chamadas telefónicas recebidas e efetuadas; recurso a escutas telefónicas; entre outros. Neste caso, a violação do direito ocorre quando a utilização destes instrumentos de trabalho permite captar aspetos da vida privada dos trabalhadores que, de outra forma, não chegariam ao conhecimento da entidade empregadora.

Por fim, importa referir que a evolução tecnológica e a adesão das empresas aos mais recentes equipamentos eletrónicos, para utilização dos mesmos como instrumentos de trabalho, potenciou o surgimento de novas formas de atentar contra a privacidade dos trabalhadores[88], designadamente através da colocação de câmaras dissimuladas no local de trabalho, da instalação de programas ocultos nos computadores da empresa, do acesso ao e-mail ou motor de busca dos trabalhadores, entre outras condutas.

Apesar de, regra geral, a utilização destes meios ter em vista um incremento do controlo exercido pelo empregador sobre os trabalhadores, a verdade é que permite captar informações da vida privada daqueles que, além de serem irrelevantes por não estarem relacionadas com o vínculo laboral, não foram partilhadas com o consentimento dos trabalhadores. Por isso, o grande problema destas práticas é que, muito embora algumas possam ter finalidades legítimas e sejam usadas em cumprimento da legislação existente, as mesmas podem ser altamente intrusivas na vida privada dos trabalhadores, deixando-os totalmente "a descoberto" perante a entidade empregadora, o que reduz excessivamente a dignidade da sua pessoa[89]. Por esse motivo, as

Jorge Ribeiro de Faria, 2003, p. 664-669 [Cons. 18 mar. 2021] Disponível em: <https://repositorio-aberto.up.pt/bitstream/10216/24325/2/49769.pdf>.

87 Cfr. Catarina Sarmento E Castro, *A proteção de dados pessoais dos trabalhadores*, in Questões Laborais, Ano IX -Nº 20, 2002, Coimbra Editora, ISSN 0872-8267, p. 139-145.

88 A este respeito, v. Manuel Luque Parra e Francisco Ramón Lacomba, *Acceso a dispositivos digitales del trabajador*, in Vigilancia y control..., p. 358.

89 Para uma análise mais detalhada sobre as técnicas habitualmente usadas pelos empregadores, v. Tom Wright, *Workplace Privacy: A Consultation Paper*, Information and Privacy Commissioner, 1992, p. 3-20 [Cons. 18 mar. 2021] Disponível em: <https://silo.tips/download/workplace-privacy-a-consultation-paper>.

condutas levadas a cabo pela entidade empregadora, sem dar conhecimento ou pedir o consentimento dos trabalhadores para tal, padecem de ilicitude.

Assim, parece-nos que a melhor forma de resolver este conflito sempre será a de ambas as partes nortearem a sua atuação pelo princípio da boa-fé[90], conforme preveem os artigos 102º e 126º do CT, o que implica dar a conhecer aos trabalhadores toda e qualquer forma de controlo e vigilância que o empregador empregue e que possa captar informações da sua vida privada.

Porém, a questão que ora se levanta é a de saber se as constantes intromissões na vida privada dos trabalhadores são admissíveis mediante autorização daqueles, isto é, em que medida é que o direito à reserva da vida privada pode sofrer restrições, com fundamento na disponibilidade do mesmo por parte dos seus titulares.

4. DISPONIBILIDADE

Como refere Jean Rivero[91], o contrato de trabalho pressupõe «da parte do trabalhador uma renúncia parcial à sua liberdade» que pode ocorrer de duas formas: através de disposições legais que limitam a atuação do trabalhador no tempo e local de trabalho (de que são exemplo os deveres dos trabalhadores) ou mediante a disponibilidade de direitos levada a cabo pelos trabalhadores.

No que respeita à disponibilidade, importa referir que, regra geral, a constituição ou extinção de relações jurídicas e, bem assim, a aquisição ou a perda de direitos depende da vontade das partes[92]. Contudo, existem direitos que não estão na disponibilidade das partes (indisponíveis) ou que apenas o estão parcialmente (relativamente indisponíveis).

O direito à reserva da vida privada, que resulta da lei, não é um direito absoluto nem totalmente indisponível, pelo que, em determinadas situações, este direito dos trabalhadores pode ceder perante os interesses legítimos do empregador[93]. Contudo, e uma vez que se trata de um direito de personalidade, o direito à reserva da vida privada é irrenunciável, o que significa que os trabalhadores não podem abdicar dele na totalidade, mas apenas limitar o exercício do seu direito[94] para determinado fim. Assim, o direito à reserva da vida privada é um direito relativamente disponível.

---

90 Cfr. Teresa Alexandra Coelho Moreira, *A Privacidade dos Trabalhadores...,* p. 386-391.

91 Cfr. Jean Rivero, *Les libertés publiques dans l'entreprise*, in DS, nº 5, 1982, p. 422 Apud. Teresa Alexandra Coelho Moreira, *Da Esfera Privada do Trabalhador…*, nota 440.

92 Cfr. João De Castro Mendes, *Direito Processual Civil*, vol. I, ed. rev. e act., Lisboa, AAFDL Editora, 1987, ISBN 5606939000774, p. 210-213.

93 Cfr. Jeremy De Beer, *Employee Privacy…*, p. 384.

94 Cfr. Teresa Alexandra Coelho Moreira, *A Privacidade dos Trabalhadores...*, p. 310.

4.1. PRINCÍPIO DA IRRENUNCIABILIDADE

Antes de mais, importa referir que, embora possam existir outras conceções de renúncia, neste trabalho abordamos a renúncia enquanto forma de abdicar de um direito, tal como a configura Francisco Pereira Coelho[95]. Assim, quando o titular de um direito renuncia ao mesmo, produzem-se os seguintes efeitos: extinção subjetiva do direito (efeito imediato), extinção objetiva e atribuição de uma vantagem (efeitos legais ulteriores).

No caso do direito à reserva da vida privada, por exemplo, a renúncia abdicativa levada a cabo pelo trabalhador teria como efeito a extinção da proteção que a ordem jurídica lhe confere (eficácia extintiva/abdicativa) e, ao mesmo tempo, atribuiria ao empregador a possibilidade de conhecer informações da sua vida privada (eficácia atributiva).

Sucede que, através da renúncia abdicativa, não só se assume a obrigação de não exercer o direito, como se extingue esse direito na esfera jurídica do titular, o que não é permitido quanto ao direito à reserva da vida privada, conforme já referimos.

Na relação laboral, que é uma relação de direito privado, continua a vigorar o princípio da autonomia privada, que confere às partes disponibilidade para regularem a relação jurídica existente entre elas. Contudo, e atentas as vicissitudes do contrato de trabalho, especialmente no que respeita ao desequilíbrio de poderes de ambas as partes, existem alguns normativos legais de índole imperativa que procuram salvaguardar os direitos dos trabalhadores, conferindo-lhes o caráter de irrenunciáveis[96].

Assim, e subscrevendo Guy Davidov[97], podemos dizer que vigora na relação laboral um princípio da irrenunciabilidade, que se traduz na limitação da disponibilidade de determinados direitos pelos trabalhadores e que tem em vista proteger estes últimos de atuarem com base num ato de manifestação de vontade que não é totalmente livre e, dessa forma, abdicarem de direitos que a legislação laboral lhes confere.

No nosso ordenamento jurídico, e mais concretamente no CT, são várias as normas que evidenciam a existência de um princípio de irrenunciabilidade. A título de exemplo, veja-se o caso do direito a férias, que é irrenunciável por força dos arts. 237º, nº 3 do CT e 59º, nº 1, *al. d),* da CRP, embora os trabalhadores possam renunciar ao gozo integral do período de férias, nos termos do art. 238º, nº 5 do CT. Da mesma forma, o direito à retribuição é

---

95 Cfr. Francisco Manuel De Brito Pereira Coelho, *A Renúncia Abdicativa no Direito Civil: algumas notas tendentes à definição do seu regime*, Coimbra Editora, 1995, Studia Iuridica 8, ISBN 972-32-0687-0, p. 7-60.

96 Cfr. Pedro Romano Martinez, *Direito do Trabalho...*p. 276 e 277.

97 Cfr. Guy Davidov, *Nonwaivability in Labour Law*, Oxford Journal of Legal Studies (forthcoming), 2020, p. 1 [Cons. 2 abr. 2021] Disponível em:<https://www.academia.edu/42344619/Nonwaivability_in_Labour_Law>.

irrenunciável, mas existe a possibilidade de cessão de crédito nos termos do art. 280º do CT.

Se considerarmos que a renúncia constitui uma auto-restrição levada a cabo pelo titular do direito, parece que o princípio da irrenunciabilidade restringe o direito à autonomia privada dos trabalhadores[98]. Contudo, não é verdadeiramente assim, pois a irrenunciabilidade protege a autonomia dos trabalhadores tomarem decisões livres, sem qualquer coação.

Ora, se atendermos à desigualdade existente entre as partes contratuais na relação laboral e aos interesses que subjazem à atuação de uma e outra, facilmente compreendemos a importância do princípio da irrenunciabilidade nesta relação. Portanto, mesmo que seja o trabalhador a dispor do seu direito à reserva da vida privada, é necessário averiguar se o próprio não estará a fazer uma restrição excessiva do seu direito ou a até a renunciar àquele, não por ser essa a sua vontade, mas por razões externas.

Neste sentido, Guy Davidov defende que a desigualdade existente entre o trabalhador e a sua entidade empregadora justifica a existência de uma presunção a favor do trabalhador, segundo a qual qualquer renúncia de direitos por parte do trabalhador terá por detrás uma imposição ou, pelo menos, um incentivo do empregador, sendo que essa presunção só poderá ser afastada mediante a prova em contrário por parte do empregador[99].

Apesar disso, têm-se verificado cada vez mais situações nas quais os trabalhadores renunciam aos seus direitos laborais, na expectativa de obterem uma contrapartida. Aliás, nos dias que correm, uma grande parte da informação relativa à vida privada dos trabalhadores fica disponível porque estes a disponibilizam voluntariamente ou de forma inconsciente. Tal acontece facilmente na internet, com o uso das redes sociais, mas também na relação de trabalho, na qual o trabalhador consente que o empregador tome conhecimento de informações que integram a sua vida privada ou ele próprio disponibiliza essas informações.

Essa tendência poderia justificar o raciocínio de que, se o trabalhador autoriza que a entidade empregadora aceda às informações, então não teria sentido invocar, nesses casos, o direito à reserva da vida privada. É precisamente isso que se tem entendido quando o trabalhador coloca as informações nas redes sociais, acessíveis a todos[100].

De facto, o exercício do direito à reserva da vida privada inclui a possibilidade de escolher, isto é, a autonomia de tomar decisões, o controlo pelo

---

98 Cfr. Guy Davidov, *Nonwaivability in Labour Law…*, p. 4-10.

99 Cfr. Guy Davidov, *Nonwaivability in Labour Law…,* p. 2 e 21.

100 Neste sentido, v. Diogo Figueiredo Perfeito Dias Ferreira, *Trabalhador, Reserva…*, p. 595-599.

titular do direito da sua informação pessoal e dos seus direitos, bem como a delimitação do seu espaço físico[101] .

Neste sentido, admitimos a existência de um princípio da irrenunciabilidade, mesmo quando a vontade dos trabalhadores seja diversa da proteção conferida por esse princípio, podendo, no entanto, existir soluções intermédias de disponibilidade limitada, que pressuponham uma escolha livre, totalmente informada e racional[102].

Alguns exemplos de disponibilidade limitada que constam do nosso CT são: a estrutura hierárquica das fontes de direito do trabalho (art. 3º CT); a proibição de disposições de regulamentação coletiva de trabalho contrárias ao princípio da igualdade e não discriminação (art. 26º CT); o período experimental opcional e o limite de duração (art. 111º ss CT); os requisitos para a mobilidade funcional (art. 120º, nº2 CT); as regras específicas para a contratação a termo (art. 139º ss CT e 53º CRP); a limitação dos tempos de trabalho (art. 197º ss CT); a taxatividade das formas de cessação do contrato de trabalho (arts. 338º ss CT); e o princípio do tratamento mais favorável (art. 476º CT).

Caraterística comum a todos estes exemplos é o facto de o legislador ter colocado essas matérias na disponibilidade das partes, embora limitando as possibilidades de escolha e impondo restrições à opção por vias que possam ser menos favoráveis para os trabalhadores.

4.2. LIMITAÇÃO VOLUNTÁRIA DO DIREITO

Partindo da ideia de que é possível limitar o gozo do direito, mas não renunciar ao mesmo, Paulo Mota Pinto apresenta-nos a disponibilidade do direito à reserva da vida privada como uma autolimitação desse direito, levada a cabo pelo seu titular. Para tal, este autor começa por distinguir a limitação voluntária da reserva da vida privada através do consentimento da configuração que o titular do direito faz da sua vida privada[103].

Mediante os seus interesses e personalidade, os trabalhadores delimitam o objeto da sua vida privada, definindo o que é público e o que é privado na sua perspetiva. Assim, quando consentem com uma limitação da sua vida privada e disponibilizam ou permitem o acesso a determinadas informações que a integram, os trabalhadores estão a autolimitar esse objeto de privacidade que foram construindo na sua vida, do qual fazem parte as informações que os mesmos querem manter para si ou partilhar com um círculo restrito de pessoas.

---

101 São as chamadas "quatro esferas de privacidade", identificadas por JON L. MILLS. (Cfr. Jon L. Mills, *Privacy: the lost right*, Oxford University Press, Inc., 2008, ISBN 978-0-19-536735-5, p. 105 ss)

102 Cfr. Guy Davidov, *Nonwaivability in Labour Law…*, p. 18-24.

103 Cfr. Paulo Mota Pinto, *Direitos de Personalidade...,* P. 633-634 e 687 ss.

Por isso, entendemos como Mota Pinto que a conformação do direito pelo seu titular não constitui uma forma de limitação voluntária do direito, pois a conformação tem a ver com a definição do objeto do direito, enquanto que a limitação recai sobre o objeto já definido[104].

Assim, a disponibilidade do direito à reserva da vida privada levada a cabo pelos trabalhadores consiste na faculdade de estes limitarem o gozo desse direito, cuja amplitude será menor ou maior conforme a delimitação feita pelos próprios da sua vida privada, mas sem renunciarem ao direito, nem ultrapassarem o mínimo de proteção que a lei lhes confere.

Posto isto, a limitação voluntária do direito à reserva da vida privada pode ocorrer de duas formas: através da divulgação de informações pelo titular do direito; ou mediante o consentimento do titular para que a entidade empregadora aceda a essas informações. Ambas as hipóteses consubstanciam uma manifestação da autonomia privada enquanto «poder de livre exercício dos seus direitos ou de livre gozo dos seus bens pelos particulares»[105].

4.3. CONSENTIMENTO

A forma através da qual os trabalhadores dispõem do seu direito à reserva da vida privada é através do consentimento, por meio do qual aqueles autorizam a sua entidade empregadora a aceder a informações relativas à sua vida privada, a utilizar meios de vigilância que captam aspetos da vida privada, a tratar os dados e informações que os próprios trabalhadores facultam e, se necessário, a transmiti-los a determinadas entidades.

Assim, e tendo em consideração o caráter lato do direito à reserva da vida privada, bem como a possibilidade de auto conformação e de disponibilidade parcial do mesmo, o consentimento tem sido encarado por vários autores como o fator decisório para aferir da licitude ou ilicitude das práticas que atentem contra a reserva da vida privada dos trabalhadores.

Conforme referem Orlando de Carvalho[106] e, na sua esteira, Paulo Mota Pinto[107], o consentimento pode assumir diferentes modalidades: consentimento tolerante, consentimento autorizante e consentimento vinculante.

Pese embora surjam no Direito Civil, estas modalidades do consentimento podem ser transpostas para a relação laboral. Assim, o consentimento tolerante corresponde às situações em que os trabalhadores se apercebem de uma agressão ao seu direito e a toleram, nada fazendo. Por sua vez, o consentimento autorizante diz respeito à declaração de consentimento emitida pelo trabalhador, que permite à entidade empregadora atentar contra o

---

104 Cfr. Paulo Mota Pinto, *Direitos de Personalidade…*, p. 684-686.

105 Cfr. Carlos Alberto Da Mota Pinto [et. al.], *Teoria Geral do Direito Civil*, 5ª ed., Coimbra, Gestlegal, 2020, ISBN 978-989-8951-53-3, p. 103.

106 Cfr. Orlando De Carvalho, *Teoria Geral ...*, p.205.

107 Cfr. Paulo Mota Pinto, *Direitos de Personalidade…,* p. 708-712.

seu direito. Este consentimento é revogável a todo o tempo e não vincula o titular do direito. Já o consentimento vinculante corresponde a uma obrigação assumida pelo trabalhador, que atribui à entidade empregadora um direito e se equipara a um negócio jurídico.

Das três modalidades de consentimento apresentadas, iremos focar o objeto do presente estudo no consentimento autorizante, cujas caraterísticas analisaremos de seguida.

a) Conceito

Até há bem pouco tempo, o consentimento era visto como uma declaração negocial, nos termos e para os efeitos dos artigos 217º e ss do CC. Nesse sentido, toda e qualquer área do saber ia buscar a noção de consentimento ao Código Civil, à Teoria Geral do Direito Civil.

O consentimento era interpretado como uma manifestação de vontade através da qual o titular do direito exteriorizava as suas pretensões, sem prejuízo de se reconhecer que, em algumas situações, a vontade declarada poderia não corresponder à vontade real, caso existisse algum vício da vontade[108].

Contudo, o Regulamento Geral de Proteção de Dados (Regulamento UE n.º 679/2016, de 27 de Abril) veio romper com essa concepção de consentimento e foi inovador, pois apresentou um conceito mais desenvolvido e com novas vicissitudes[109], reforçando que o ponto fulcral do consentimento é a manifestação da vontade.

b) Requisitos de validade e integridade

Sendo o consentimento para limitação voluntária do direito à reserva da vida privada dos trabalhadores uma declaração negocial, o mesmo tem que obedecer a determinados requisitos para ser considerado válido.

Antes de mais, o consentimento dos trabalhadores está sujeito aos princípios da liberdade da declaração e da liberdade de forma, previstos nos arts. 217º, nº1 e 219º do CC, respetivamente[110] . Apesar disso, o RGPD operou uma mudança de paradigma e veio impor que o consentimento seja um

---

[108] Sobre a declaração negocial, v. Carlos Alberto Da Mota Pinto [et. al.], *Teoria Geral*, p. 413-440.

[109] No artigo 4º, nº11 do RGPD pode ler-se que o consentimento consiste numa «manifestação de vontade livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento» Cfr. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>.

[110] Cfr. Paulo Mota Pinto, *Direitos de Personalidade…*, p. 693.

ato positivo e inequívoco[111], ao contrário do que acontecia na Diretiva anterior[112], que deixava em aberto a possibilidade de o consentimento resultar de uma não ação, isto é, de uma omissão.

Acresce que o consentimento é uma declaração de vontade receptícia, pelo que o consentimento para o acesso do empregador a informações da vida privada dos trabalhadores terá sempre que ser prévio, ou seja, terá que ser manifestado pelos trabalhadores em momento anterior ao da consumação da ofensa à vida privada daqueles.

Além disso, o consentimento não pode ser presumido[113], mas antes tem que ser expresso e manifestado para cada situação específica, portanto terá que ser dado com um limite temporal que, no caso da relação laboral, poderá ser a vigência do contrato de trabalho.

Ademais, o consentimento para ser válido tem que ser legal, consciente e esclarecido, sendo ponderados todos os efeitos da limitação do direito[114]. Por esse motivo, o consentimento dos trabalhadores não pode ser geral, mas antes tem que estar estritamente delimitado (identificados os factos para os quais se consente, quais as finalidades e a duração do acesso e do tratamento dessas informações), pois só assim os trabalhadores poderão discernir sobre as vantagens e desvantagens de consentirem. A título de exemplo, Teresa Moreira refere que o mero conhecimento de que estão a ser vigiados por câmaras de vídeo instaladas no local de trabalho não é suficiente para permitir aos trabalhadores uma tomada de decisão livre e esclarecida[115].

Atualmente, o consentimento dos trabalhadores pode ser dado a título oneroso ou com alguma contrapartida monetária, na medida em que a comercialização de informações que integram a vida privada dos trabalhadores constitui uma forma de exercer esse direito.

Por fim, importa referir que o consentimento terá sempre que ser livre (traduzindo a vontade real dos trabalhadores) e informado (na medida em que o

---

111 Quanto a este ponto, o Considerando 32 do RGPD, dispõe que *«o consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral»* e ainda que «o silêncio, as opções pré validadas ou a omissão não deverão, por conseguinte, constituir um consentimento».

112 Cfr. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

113 Cfr. Maria Regina Redinha, *Da proteção da personalidade...*, p. 821.

114 Cfr. Teresa Alexandra Coelho Moreira, *A Privacidade dos Trabalhadores…* p. 311-312.

115 Cfr. Teresa Alexandra Coelho Moreira, *A Privacidade dos Trabalhadores...* , p. 479.

trabalhador deve ter conhecimento «*do caráter obrigatório ou facultativo das respostas, bem como das possíveis consequências se não responder*»[116]).

c) Efeitos

A limitação voluntária do direito à reserva da vida privada através do consentimento significa, para a entidade empregadora, a oportunidade de aceder a determinadas informações ou de colocar sistemas de monitorização eletrónica nos instrumentos de trabalho usados pelos seus trabalhadores, tomando conhecimento de aspetos que integram a reserva da vida privada dos trabalhadores e que, sem o consentimento dos mesmos, não poderiam ser conhecidos.

Porém, a questão que se coloca é a de saber se o consentimento dos trabalhadores constitui uma causa de justificação da lesão e exclui a ilicitude da atuação da entidade empregadora, ou se, por outro lado, o consentimento exclui a existência de lesão.

A este respeito, Mota Pinto[117] entende que o consentimento dos trabalhadores constitui um acordo na limitação voluntária do seu direito e, por esse motivo, afasta a lesão, tornando impossível recorrer aos meios de tutela do direito que exijam a ilicitude como pressuposto. Não podemos concordar com essa afirmação, pois tal seria extremamente desvantajoso para os trabalhadores, na medida em que diminuiria bastante as suas possibilidades de reação. Assim, consideramos que o acesso da entidade empregadora às informações da reserva da vida privada dos trabalhadores constitui sempre um ato lesivo e que o consentimento dos trabalhadores poderá funcionar como uma causa de justificação da lesão, excluindo a ilicitude[118]. Aliás, parece ser isso mesmo que decorre do artigo 340º do CC.

d) Revogação do consentimento

Conforme consta do art. 81º, nº 2 do CC, a limitação voluntária do direito à reserva da vida privada mediante o consentimento do titular do direito é revogável a todo o tempo e de forma livre, sem prejuízo de o trabalhador ter que indemnizar a entidade empregadora, em caso de prejuízo causado pela retirada do consentimento[119]. Contudo, a obrigação de indemnizar poderá não existir se o consentimento do trabalhador for declarado nulo por violação de uma proibição legal ou da ordem pública[120].

---

116 Cfr. Catarina Sarmento E Castro, *Questões Laborais*, Ano IX, nº 19, Coimbra Editora, 2002, ISSN 0872-8267, p. 59.

117 Cfr. Paulo Mota Pinto, *Direitos de Personalidade…*, p.688-689.

118 Cfr. Maria Regina Gomes Redinha, *Direitos de personalidade …*, p. 3.

119 Cfr. Teresa Alexandra Coelho Moreira, *A Privacidade dos Trabalhadores*, p. 312.

120 Cfr. Paulo Mota Pinto, *Direitos de Personalidade…*, p.713.

4.4. DISPONIBILIDADE (IN)VOLUNTÁRIA

Aquilo a que assistimos muitas vezes, em especial nas relações de trabalho em que os trabalhadores têm um baixo nível de escolaridade, são mais velhos ou têm uma maior dependência económica, é que a entidade empregadora conhece as fragilidades dos mesmos e consegue obter todas as informações que pretende sobre a sua vida privada, uma vez que, em virtude da subordinação jurídica e da dependência económica que subjazem àquela relação, os trabalhadores consideram que prestar informações sobre a sua vida privada à entidade empregadora constitui uma obrigação contratual. Assim, coloca-se a questão de saber se, ao celebrar o contrato, está implícito que o trabalhador aceita partilhar com a sua entidade empregadora aspetos da sua vida privada.

Considerando o poder de direção do empregador, alguns autores tendem a reconhecer, nesta fase, um consentimento implícito do trabalhador, que confere ao empregador autorização para tratar questões diretamente relacionadas com a relação laboral, limitando a sua privacidade[121]. A nosso ver, esta argumentação não tem muito sentido, pois ao trabalhador apenas é exigível partilhar com o seu empregador as informações estritamente necessárias para a execução do contrato, pelo que o consentimento deve ser sempre explícito e obedecer a todos os requisitos de validade supramencionados.

Apesar disso, continuam a verificar-se inúmeros casos nos quais a entidade empregadora solicita informações da vida privada aos seus trabalhadores, invocando para tal que necessita dessas informações para a execução dos contratos. Ora, a relação de confiança existente entre ambas as partes e o facto de os trabalhadores não estarem devidamente esclarecidos sobre os direitos que lhes assistem levam a que, na maior parte das vezes, os trabalhadores consintam o acesso a determinados dados da sua vida privada ou sejam eles próprios a facultá-los, considerando, com isso, estar a cumprir o contrato. Assim, questiona-se se é possível invocar o direito à reserva da vida privada quando foi o próprio titular do direito a disponibilizar a informação ou consentir o acesso[122].

A este respeito, é de notar que, na relação laboral, a integridade do consentimento é questionável, na medida em que a desigualdade existente entre as partes leva a que se coloque em causa a vontade efetiva dos trabalhadores que dão o seu consentimento para intrusões na sua esfera privada levadas a cabo pela entidade empregadora[123]. Desde logo porque, se os trabalhadores não compreendem quais as informações que têm que partilhar

---

121 Cfr. Teresa Alexandra Coelho Moreira, *A Privacidade dos Trabalhadores...*, p. 330.

122 Cfr. Diogo Figueiredo Perfeito Dias Ferreira, *Trabalhador…*, p. 598 e Paulo Mota Pinto, *Direitos de Personalidade…*, p. 694.

123 Neste sentido, Jesús Cruz Villalón, *El impacto de la digitalización sobre los derechos fundamentales laborales*, in Vigilancia y control..., p. 66. Perfilhando o mesmo entendimento, Teresa Alexandra Coelho Moreira, *A Privacidade dos Trabalhadores…,* p. 480.

e quais devem reservar para si, a tendência será sempre a de partilharem as informações que lhes pedem ou consentirem no acesso às mesmas, sob pena de sofrerem represálias no vínculo laboral.

Foi neste sentido que o RGPD procedeu à necessária distinção do consentimento dado na relação laboral, considerando que, por se tratar de uma relação jurídica na qual existe uma grande desigualdade entre as partes[124], o consentimento dos trabalhadores é mais frágil do que o consentimento emitido noutras relações jurídicas[125].

Contudo, a falta de resposta ou a recusa dos trabalhadores em prestar determinadas informações que integram a sua vida privada, por exemplo, são atitudes mal recebidas pela maior parte das entidades empregadoras, que as consideram uma afronta ao seu poder. Assim, a manifestação da vontade real dos trabalhadores, no sentido de não darem o seu consentimento e não disporem, por qualquer forma, do seu direito à reserva da vida privada, resulta inúmeras vezes em repercussões para os trabalhadores, de que são exemplo a aplicação de sanções disciplinares, perda de benefícios, assédio laboral e até despedimentos.

Posto isto, consideramos que a mera circunstância de ter existido consentimento dos trabalhadores não basta para se afastar a ilicitude da ofensa ao direito à reserva da vida privada, na medida em que, muitas vezes, esse consentimento não é completamente livre[126] . Além disso, propendemos a considerar, como Guy Davidov, que se não podemos saber quando uma escolha é livre e quando não o é, mas temos motivos para acreditar que na

---

[124] No considerando 43 do RGPD pode ler-se: «A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento.»

[125] Assim, a Lei de de Execução Portuguesa veio estipular no art. 28º, nº3 que «salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais» nos casos previstos nas al. a) e b) desse mesmo art. Contudo, a CNPD, na Deliberação 2019/494, veio desaplicar essa norma por considerar que esta disposição traduz uma restrição injustificada e desproporcionada do disposto na alínea a) do n.º 1 do artigo 6.º e da alínea a) do n.º 2 do artigo 9.º do RGPD, argumentando que decorre do princípio da dignidade da pessoa humana a necessidade de reconhecer ao indivíduo o mínimo de livre-arbítrio para decidir sobre os dados que lhe digam respeito. Apesar disso, o GT 29 optou por recusar relevância jurídica ao consentimento dos trabalhadores, embora considerando que estes possam dar o seu consentimento livremente em circunstâncias excecionais, quando o ato de dar ou recusar o consentimento não produza quaisquer consequências negativas, ressalvando que o elemento "livre" implica uma verdadeira escolha e controlo para os titulares dos dados e que, por isso, se o titular dos dados não puder exercer uma verdadeira escolha, se se sentir coagido a dar o consentimento ou sofrer consequências negativas caso não consinta, então o consentimento não é válido. Cfr. Guidelines on Consent under Regulation 2016/679 [Cons. 30 mai. 2021] Disponível em: <https://ec.europa.eu/newsroom/article29/items/623051>.

[126] Quanto a este tema, v. Catarina Sarmento E Castro, *Questões Laborais… parte 1*, p.58.

maior parte dos casos não é livre, faz sentido criar uma regra baseada na hipótese mais comum[127].

Assim, deverá ser possível avaliar a integridade do consentimento casuisticamente, tendo em consideração as circunstâncias que motivaram o consentimento[128] e mantendo à disposição dos trabalhadores os mecanismos de defesa do seu direito à reserva da vida privada, entre os quais a possibilidade de anulação ou declaração de nulidade do consentimento[129], com fundamento na existência de algum vício de vontade, na ilicitude do consentimento ou ainda na contrariedade da ordem pública.

4.5. LIMITES INTRANSPONÍVEIS

Analisada a forma como, habitualmente, os trabalhadores dispõem do seu direito à reserva da vida privada, importa referir que a validade dessa disponibilidade depende do respeito por determinados limites, que são intransponíveis.

Em primeiro lugar, a disponibilidade do direito à reserva da vida privada terá que ser parcial, na medida em que não é possível dele dispor totalmente, renunciando a esse direito[130].

Em segundo lugar, essa disponibilidade do direito não significa que o empregador esteja autorizado a utilizar indiscriminadamente as informações obtidas, desde logo porque a disponibilidade deverá ter sempre subjacente uma finalidade específica.

Em terceiro lugar, não é admissível que a disponibilidade coloque em causa a dignidade do trabalhador enquanto pessoa. Se tal acontecer, considera-se que o direito é indisponível.

Além disso, para haver uma restrição do direito à reserva da vida privada dos trabalhadores, terá que se invocar o critério da proporcionalidade, previsto no art. 18º, nº 2 da CRP, que se desdobra em três dimensões: a necessidade, a adequação e a proporcionalidade em sentido estrito. Assim, para cada situação concreta, deverá averiguar-se se a restrição do direito à reserva da vida privada é necessária para a execução do contrato ou para o bom funcionamento da empresa, bem como se essa restrição permite atingir os resultados esperados, e ainda se não existia outra forma, menos one-

---

127 Cfr. Guy Davidov, *Nonwaivability in Labour…*, p. 7-8.

128 A este respeito, GUY DAVIDOV sugere que a análise da validade e da voluntariedade do consentimento inclua elementos subjetivos (compreender o pensamento do trabalhador ao fazer aquela escolha) e elementos objetivos (visão social sobre que circunstâncias contribuíram para uma escolha livre). Cfr. Guy Davidov, *Nonwaivability in Labour…*, p.7-10.

129 Como refere MOTA PINTO, a anulação do consentimento poderá justificar-se quando este contrarie uma disposição imperativa. (Cfr. Paulo Mota Pinto, *Direitos de Personalidade…,* p. 702)

130 Neste sentido, v. Paulo Mota Pinto, *Direitos de Personalidade…*, p. 634.

rosa para os trabalhadores, de alcançar esses objetivos, sem limitar os seus direitos e os expor a riscos desnecessários[131].

Acresce que o arts. 81º, nº 1 e 280º, nº 2 ambos do CC proíbem a limitação voluntária dos direitos de personalidade, quando esta for contrária aos princípios de Ordem Pública. Ora, como refere Maria Raquel Guimarães[132], a ordem pública tem caráter subsidiário, pelo que apenas deverá ser invocada em *ultima ratio*, quando não existir mais nenhum preceito capaz de salvaguardar o bem jurídico em perigo e de proibir comportamentos que o lesem.

Assim, será um importante meio de defesa do direito à reserva da vida privada naquelas situações que, não estando reguladas ou nunca tendo sido suscitadas, possam emergir em virtude das frequentes mutações da relação laboral, tornando necessária uma atuação díspar, sob pena de não se conseguir alcançar a justiça social nesses casos. A título de exemplo, podemos apontar os casos em que o consentimento dos trabalhadores for inespecífico, irrevogável, ou contrariar uma norma imperativa[133].

5. EFETIVAÇÃO

5.1. INTERVENÇÃO DO ESTADO COMO GARANTE DO EQUILÍBRIO NA RELAÇÃO LABORAL

Ao longo deste trabalho, defendemos a existência de uma desigualdade entre as partes contratuais na relação laboral e, consequentemente, sustentamos a necessidade de proteger os trabalhadores, o que implica por vezes uma limitação da sua autonomia, designadamente através do princípio da irrenunciabilidade e da anulabilidade do consentimento.

A este respeito, e secundando D. Leite Campos, importa relembrar que a autonomia privada se traduz na faculdade que cada pessoa tem de estabelecer relações jurídicas com os outros, celebrando negócios jurídicos, quando, como e com quem quiser, de acordo com os seus interesses[134].

Sucede que, na relação laboral, estas ideias não têm efetivação tal e qual como são concebidas. Em primeiro lugar porque se trata de um contrato do qual depende a subsistência ou realização pessoal das pessoas, no qual acabam por pesar muitos mais fatores do que a mera vontade de contratar,

---

131 Quanto a este ponto, v. Teresa Alexandra Coelho Moreira, *A Privacidade dos Trabalhadores…,* p. 520-534 e ainda Maria Regina Gomes Redinha, *Direitos de personalidade...,* p. 4.

132 Cfr. Maria Raquel Guimarães, *A Conformação da Liberdade Contratual pela Cláusula Geral da Ordem Pública,* in Derecho y Autonomía Privada: Una Visión Comparada e Interdisciplinar, Editorial Comares, S.L., Granada, 2017, ISBN 978-84-9045-521-0, p. 418.

133 Cfr. Paulo Mota Pinto, *Direitos de Personalidade…*, p. 701-703.

134 Cfr. Diogo Leite De Campos, *Lições de direitos…*, p. 103.

sendo na maior parte das vezes uma necessidade. Em segundo lugar, porque são raros os contratos de trabalho nos quais os trabalhadores têm uma palavra a dizer sobre as cláusulas e os demais termos contratuais, sendo antes colocados perante contratos redigidos pela entidade empregadora e face aos quais a única escolha que fazem verdadeiramente é a de aceitar ou não aceitar o trabalho em questão.

Assim, se a autonomia privada está, em regra, intimamente ligada ao direito de não ficar subordinado a outro ser humano, sendo aliás uma manifestação dessa liberdade, aquilo que se verifica na relação laboral é o oposto, pois é precisamente através da autonomia privada que os trabalhadores se colocam numa posição de subordinação perante outrem.

Posto isto, entendemos que, na relação de trabalho, se verifica uma inversão do sentido original que se pretendeu dar à autonomia privada, enquanto forma de realização pessoal e de liberdade, o que justifica a função protecionista do direito do trabalho[135]. E, nesse sentido, consideramos ser importante a intervenção estatal, designadamente através de atos legislativos que confiram especial proteção aos trabalhadores, atuando o Estado como garante do equilíbrio entre os poderes do empregador e os direitos dos trabalhadores.

A intervenção estatal no âmbito laboral foi tendo sempre um de dois objetivos: a proteção dos trabalhadores ou a proteção dos interesses empresariais[136]. O primeiro objetivo tinha em vista proteger os trabalhadores perante a desigualdade económica e conceder-lhes condições de trabalho dignas, o que aconteceu através da criação do salário mínimo nacional e da legislação de segurança e saúde no trabalho, por exemplo. Já o segundo objetivo prende-se com a gestão empresarial com vista ao crescimento económico.

Apesar de ambas as perspetivas nortearem a intervenção do Estado no âmbito do direito do trabalho, somos de opinião que, nos dias de hoje, este intervencionismo se deve cingir a conferir proteção aos trabalhadores enquanto parte mais frágil na relação laboral, cabendo ao Estado a tarefa de, através da legislação laboral, diminuir as desigualdades e proteger aqueles que habitualmente se encontram mais desprotegidos. Aliás, a intervenção estatal deverá limitar-se ao mínimo possível, de modo a não retirar efetividade aos princípios da autonomia privada e da liberdade contratual, caraterísticos do direito privado, nem diminuir o livre arbítrio das pessoas na tomada de decisões.

A nosso ver, é este intervencionismo que está na génese das normas imperativas e do princípio da irrenunciabilidade que vigoram na relação laboral, procurando limitar o poder decisório dos trabalhadores em questões que dizem respeito à garantia da dignidade humana.

---

135 Cfr. José João Nunes Abrantes, C*ontrato de Trabalho...*, p. 36-44.

136 Cfr. John D.R. Craig, *Privacy & Employment Law,* Hart Publishing, Oxford and Portland, Oregon, 1999, ISBN 1-84113-059-1, p. 41.

Da mesma forma, parece ter sido esse o propósito do legislador europeu na elaboração da Diretiva Transparência[137], que veio alargar o âmbito do dever de informação na pessoa do empregador, obrigando a que este esclareça o trabalhador sobre uma série de informações relativas ao vínculo laboral. Reconhecendo as desigualdades existentes na relação laboral e a dificuldade acrescida de os trabalhadores exercerem os seus direitos quando não os conhecem detalhadamente, o legislador europeu consagrou a obrigatoriedade de a entidade empregadora prestar informações mais pormenorizadas e concretas aos trabalhadores, comunicando-lhes quais são os seus direitos ao longo da relação laboral. Assim, a Diretiva (UE) 2019/1152 poderá ter um impacto significativo no consentimento dos trabalhadores, na medida em que trabalhadores mais informados terão um maior discernimento na decisão de consentir numa limitação dos seus direitos, entre os quais o direito à reserva da vida privada. Por isso, esta Diretiva traduz uma valorização do consentimento dos trabalhadores, que ganha novos contornos e outra credibilidade se a entidade empregadora cumprir escrupulosamente o dever de informação ali configurado.

Pese embora esta intervenção estatal como forma de equilibrar a relação laboral possa ser entendida como desnecessária por muitos autores, somos de opinião contrária, pois trata-se da principal forma de proteger e dar efetivação aos direitos de personalidade dos trabalhadores que, embora inerentes a todas as pessoas, são por vezes menosprezados nas relações jurídicas.

Sem prejuízo, registam-se com frequência situações nas quais a entidade empregadora faz tábua rasa da legislação laboral, por considerar que a mesma limita a sua atuação ou dificulta os seus objetivos empresariais. Por esse motivo, existem já alguns mecanismos de defesa que permitem aos trabalhadores reagir contra violações do direito levadas a cabo pelo empregador.

5.2. TUTELA JURÍDICA

Perante um direito tão abrangente e difícil de definir como a reserva da vida privada, torna-se ainda mais importante e necessária a existência de mecanismos que permitam tutelar esse direito, quer numa dimensão preventiva, quer numa dimensão sancionatória. Assim, no ordenamento jurídico português, além das normas que consagram o direito à reserva da vida privada, encontramos alguns normativos que procuram efetivar a proteção que lhe é conferida.

No que respeita à dimensão preventiva, temos os preceitos constitucionais referidos no título 2, bem como normas de direito civil, laboral e de proteção de dados.

---

[137] Cfr. DIRETIVA (UE) 2019/1152 do Parlamento Europeu e do Conselho, de 20 de junho de 2019...

Por outro lado, a dimensão sancionatória encontra-se, por exemplo no nº 2 do art. 70º do CC, que consagra a possibilidade de aqueles que se considerarem ameaçados ou lesados no seu direito requererem uma providência que faça cessar a lesão ou a aplicação de uma sanção pecuniária compulsória ao infrator, nos termos do art. 829º-A do CC[138]. Para tal, basta fazer prova de que existe uma ameaça ou uma ofensa já consumada ao direito à reserva da vida privada, tais como o acesso indevido ou a divulgação de dados ou ficheiros pessoais[139].

Ademais, uma intromissão na vida privada pode também gerar responsabilidade civil, na primeira modalidade de ilicitude prevista no art. 483º, nº 1 do CC, sendo a culpa analisada nos termos do art. 487º, nº 2 do mesmo diploma e não se exigindo o dolo.

Por outro lado, a lesão do direito à reserva é um ato ilícito, logo permite a legítima defesa, nos termos do art. 337º do CC, desde que verificados os seus pressupostos.

Além das disposições civis, também no Código Penal português encontramos alguns normativos que tutelam o direito à reserva da vida privada, na perspetiva de reação a uma ofensa, designadamente os arts. 190º (violação de domicílio ou perturbação da vida privada), 192º (devassa da vida privada) e 193º (devassa por meio de informática).

Pelo contrário, no CT não encontramos nenhuma norma que preveja especificamente a reação dos trabalhadores face à ameaça ou à violação do seu direito à reserva da vida privada. Tal não significa, contudo, que estes não disponham de meios para reagir a estas ofensas, levadas a cabo pelo empregador, desde logo porque os trabalhadores podem recorrer aos mecanismos de tutela previstos quer na Constituição, quer na legislação civil e penal.

Além disso, o art. 17º, nº 5 do CT dispõe que constitui contraordenação muito grave o empregador exigir informações sobre a vida privada dos trabalhadores ou candidatos a emprego, quando as mesmas não sejam necessárias e relevantes para a execução do contrato.

Assim, os trabalhadores cujo direito à reserva da vida privada seja violado poderão lançar mão de alguns mecanismos tipicamente laborais, que embora não estejam previstos especificamente para essa possibilidade, constituem meios de reação adequados, entre os quais a resolução do contrato com justa causa.

---

138 MARIA REGINA REDINHA apresenta como exemplos de providências a adotar no âmbito do contrato de trabalho o afastamento do agente infrator, a transferência do trabalhador lesado para outro local de trabalho ou ainda a intimação para fazer cessar a lesão. (Cfr. Maria Regina Redinha, *Da proteção da personalidade…*, p. 821)

139 Note-se que, como refere MOTA PINTO, «o respeito pela reserva da vida privada torna, na verdade, proibidas seja a revelação ou divulgação da informação, seja a tomada de conhecimento.» (Cfr. Paulo Mota Pinto, *Direitos de Personalidade...*, p. 610)

a) Resolução do contrato com justa causa

De tudo o exposto nos capítulos anteriores resulta que as restrições desnecessárias, inadequadas ou excessivas do direito à reserva da vida privada dos trabalhadores são ilícitas[140]. Assim, se o empregador ultrapassar essa fronteira, estará a violar a esfera privada dos seus trabalhadores e, por isso, incorre em violação culposa dos seus deveres, o que consubstancia um incumprimento contratual.

Ora, dependendo do grau de violação do direito, bem como da disposição dos trabalhadores, estes poderão escolher responsabilizar o seu empregador pela infração cometida, nos termos do art. 323º do CT, ou podem optar por resolver o contrato nos termos do art. 394º, nº 2, *al. f)* do CT. Este último artigo prevê a possibilidade de o trabalhador resolver o contrato de trabalho por justa causa[141], sem cumprir o prazo de aviso prévio previsto no art. 400º do CT e ainda tendo direito a uma indemnização pelos danos sofridos, ao abrigo do art. 396º do mesmo diploma.

Conforme refere João Leal Amado[142], o artigo 394º do CT distingue entre justa causa subjetiva e justa causa objetiva. A primeira resulta de comportamentos ilícitos e culposos levados a cabo pelo empregador, de que são exemplo aqueles que estão previstos no nº 2 do artigo, embora se trate de um elenco exemplificativo. Já a justa causa objetiva pode verificar-se nos casos previstos no nº 3 do mesmo artigo, designadamente quando esteja em causa uma circunstância imputável ao trabalhador *(al. a)*, quando o empregador pratique determinados atos lícitos *(al. d)* ou atos ilícitos não culposos *(al. b)*.

Posto isto, a violação do direito à reserva da vida privada dos trabalhadores levada a cabo pela entidade empregadora consubstancia um ato ilícito culposo, que deverá ser enquadrável no art. 394º, nº 2, *al. f)* do CT, na medida em que o direito em questão consubstancia uma concretização do direito à dignidade do trabalhador.

Assim, o trabalhador que for alvo de uma violação do seu direito à reserva da vida privada por parte do empregador, de tal modo que coloque em causa a sua dignidade, dispõe de 30 dias para comunicar àquele a resolução do contrato, de acordo com o art. 395º do CT.

---

140 A este respeito, TERESA COELHO MOREIRA, defende que «a ilicitude do comportamento do empregador está na ultrapassagem realizada pelo empregador da fronteira entre a vida profissional e a vida extralaboral ou privada». (Cfr. Teresa Alexandra Coelho Moreira, *Os direitos de personalidade nas relações de trabalho*, in Direito do Trabalho: relação individual, Almedina, 2019, ISBN 978-972-40-8214-1, p. 139 e 140)

141 Note-se que, como dispõe o nº4 do art. 351º do CT, *ex vi* art. 394º, nº4 do mesmo diploma, «na apreciação da justa causa, deve atender-se, no quadro de gestão da empresa, ao grau de lesão dos interesses do empregador, ao carácter das relações entre as partes ou entre o trabalhador e os seus companheiros e às demais circunstâncias que no caso sejam relevantes».

142 Cfr. João Leal Amado, *Contrato de Trabalho…,* p. 396-401.

6. UMA ANÁLISE JURISPRUDENCIAL

Chegados aqui, importa perceber se os desenvolvimentos legislativos que se verificam em torno do direito à reserva da vida tiveram repercussões a nível jurisprudencial. Para tal, iremos fazer uma breve referência a três emblemáticos Acórdãos do TEDH, bem como destacar algumas decisões judiciais de diferentes instâncias dos tribunais portugueses, que retratam bem alguns dos tópicos de discussão que desenvolvemos neste trabalho.

6.1. JURISPRUDÊNCIA DO TRIBUNAL EUROPEU DOS DIREITOS DO HOMEM

Estando o direito à reserva da vida privada previsto e protegido no artigo 8º da CEDH, o TEDH tem sido chamado a interpretar esse artigo, a fim de lhe dar efetividade e de reconhecer intrusões na vida privada das pessoas. Para tal, este tribunal tem desenvolvido uma lógica de interpretação que passa primeiro por determinar se houve alguma intromissão na vida privada da pessoa, para depois analisar se essa ingerência é proporcional.

Assim, no Acórdão *Sidabras and Dziautas vs Lithuania*[143], o TEDH foi chamado a pronunciar-se sobre a violação dos arts. 8º e 14º da CEDH. O litígio em questão dizia respeito ao despedimento de dois cidadãos lituanos por estes terem trabalhado para o ramo lituano do KGB (Serviço de Segurança Soviético) e, consequentemente, ficarem sujeitos às restrições de emprego impostas pela Lei de Avaliação do Comitê de Segurança do Estado da URSS. Inconformados com o despedimento, aqueles cidadãos intentaram uma ação administrativa contra as autoridades de informação de segurança, alegando a violação do art. 8º (respeito pela vida privada e familiar) e do art. 14º (proibição de discriminação), ambos da CEDH. Analisada a situação e a lei que impunha tal tratamento, o TEDH concluiu que havia efetivamente violação desses direitos, invocando que um tratamento diferenciado com base na informação privada de terem sido trabalhadores do KGB afetava a vida privada dos trabalhadores e gerava discriminação, desde logo porque os proibia de procurarem emprego, o que constituía uma medida desproporcionada perante os fins que se procuravam alcançar.

Já no acórdão *Bărbulescu v. Romania*[144], o trabalhador havia sido despedido por utilizar o *messenger* do *Yahoo*, criado para contactar os clientes, para conversas privadas, o que chegou ao conhecimento da entidade empregadora através da monotorização que aquela fazia do uso da internet pelos seus trabalhadores. Inconformado com o despedimento, o trabalha-

---

[143] Cfr. Ac. do TEDH, Case of Sidabras and Others v. Lithuania *(Applications nos. 50421/08 and 56213/08),* Strasbourg, 23 set. 2015 [Cons. 27 maio 2021] Disponível em: <http://hudoc.echr.coe.int/eng?i=001-155358>.

[144] Cfr. Ac. do TEDH, Case of Barbulescu v. Romania, *(Application no. 61496/08)* Strasbourg, 5 set. 2017 [Cons. 27 maio 2021] Disponível em: <http://hudoc.echr.coe.int/spa?i=001-177082>.

dor recorreu aos tribunais e o processo chegou ao TEDH com Bărbulescu a invocar que a entidade empregadora havia violado o seu direito à privacidade, previsto no art. 8º da CEDH. Pese embora a entidade empregadora de Bărbulescu tivesse alertado os seus trabalhadores de que era proibido o uso de instrumentos de trabalho para fins pessoais e os tivesse informado de que passaria a monitorizar o seu trabalho, o TEDH entendeu que o direito de privacidade de Bărbulescu havia sido violado pela entidade empregadora, uma vez que esta havia limitado excessivamente o direito à reserva da vida privada e à confidencialidade da correspondência na relação laboral. Nesse Acórdão, o TEDH considerou que os empregadores têm direito a monitorizar as comunicações dos trabalhadores e que, no caso, a expectativa de privacidade dos trabalhadores não era grande, em virtude das políticas e avisos da entidade empregadora. Porém, concluiu que, estando em causa um conflito entre o direito dos trabalhadores à privacidade e o direito do empregador a garantir o bom funcionamento da empresa, deveria aplicar-se o teste da proporcionalidade, que no caso apontava como excessiva e desproporcional a monitorização levada a cabo pela entidade empregadora.

No Acórdão *López Ribalda and Others v. Spain*[145], estava em causa a colocação de câmaras de videovigilância de forma oculta no local de trabalho, que permitiram ao empregador confirmar as suspeitas de furto que tinha relativamente aos seus trabalhadores e, consequentemente, proceder ao despedimento dos mesmos. Sucede que os trabalhadores invocaram a ilicitude do despedimento com o argumento de que a videovigilância que capturou as imagens violava o seu direito à privacidade, elencado no art. 8º da CEDH. Apesar de o Supremo Tribunal Espanhol aceitar a colocação das câmaras ocultas com base na legitimidade dos motivos da entidade empregadora, o TEDH reverteu essa decisão. Ao aplicar o teste de proporcionalidade, o TEDH considerou que o tribunal espanhol havia falhado ao equilibrar o conflito entre os direitos do empregador proteger a sua propriedade e o direito dos trabalhadores à privacidade, pois as câmaras não estavam visíveis para os trabalhadores nem para os clientes. Mais uma vez, o TEDH aplicou o critério da proporcionalidade e considerou que, apesar dos motivos legítimos do empregador (suspeita de furto), a restrição do direito não havia sido limitada ao estritamente necessário e, por isso, concluiu pela violação do direito à privacidade.

Posto isto, é bem visível que, nos três Acórdãos existiam motivos legítimos para a ingerência na vida privada dos trabalhadores levada a cabo pela entidade empregadora, mas que nenhum deles era suficientemente forte para se sobrepor ao direito à privacidade dos trabalhadores, o que só foi possível aferir com a aplicação do teste da proporcionalidade.

---

[145] Cfr. Ac. do TEDH, Case of López Ribalda and Others v. Spain (Applications nos. 1874/13 and 8567/13) Strasbourg, 17 out. 2019 [Cons. 27 mai. 2021] Disponível em: <http://hudoc.echr.coe.int/spa?i=001-197098>.

6.2. JURISPRUDÊNCIA DOS TRIBUNAIS PORTUGUESES

Apesar de grande parte das decisões jurisprudenciais existentes até à data estarem relacionadas com ações de impugnação do despedimento, verificam-se também alguns litígios relacionados com o dever de informação aquando da contratação, com o exercício do poder disciplinar do empregador durante a execução do contrato, com a utilização do correio eletrónico pelos trabalhadores e com a utilização de meios de vigilância à distância[146].

Começando pela noção de direito à reserva da vida privada, destacamos o Ac. do STJ de 25-09-2003[147], no qual se pode ler que «a tutela do direito à intimidade da vida privada desdobra-se em duas vertentes: a protecção contra a intromissão na esfera privada e a proibição de revelações a ela relativas» e ainda que a extensão desse direito deverá ser aferida «segundo as circunstâncias do caso e das pessoas», sendo que existindo conflito de direitos, poderá sofrer limitações voluntárias por parte do seu titular. Por sua vez, o Ac. do Tribunal da Relação do Porto de 11-04-2019[148], dispõe que «*o direito à reserva sobre a intimidade da vida privada, enquanto direito fundamental de personalidade, caracteriza-se juridicamente como inato, inalienável, irrenunciável e absoluto, no sentido de que se impõe, por definição, ao respeito de todas as pessoas*».

No que respeita ao dever de informação, é importante referir o Acórdão do TC nº 306/2003[149], no qual estava em causa saber se o dever de informação que recai sobre os trabalhadores implica uma restrição do seu direito à reserva da vida privada. Analisada a questão, o TC entendeu que, por força do princípio geral de proibição da exigência de informações relativas à vida privada, os trabalhadores não tinham que partilhar informações relativas ao estado de saúde e gravidez. Nesse sentido, o empregador não tinha o direito de indagar os candidatos a emprego sobre aquelas questões, a menos que se verificasse alguma das exceções previstas na lei e que fundamentasse, por escrito, essa pretensão. Por isso, o TC decidiu pela «inconstitucionalidade do acesso direto do empregador» a essas informações *«por violação do princípio da proibição do excesso nas restrições ao direito fundamental à reserva da intimidade da vida privada, decorrente das disposições conjugadas dos*

---

146 Cfr. Maria Do Rosário Palma Ramalho, *Tutela da personalidade...*, p. 10-16.

147 Cfr. Ac. do Supremo Tribunal de Justiça de 25-09-2003, Proc. 03B2361 [Cons. 27 mai. 2021] Disponível em <http://www.dgsi.pt/jstj.nsf/0/0e0db401e6e9d5dc80256dea004e8bba?OpenDocument>.

148 Cfr. Ac. do Tribunal da Relação do Porto de 11-04-2019, Proc. 24733/17.3T8PRT.P1 [Cons. 27 mai. 2021] Disponível em:

<http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/d7c7bbf9d0de6091802583fa003bb587?OpenDocument>.

149 Cfr. Ac. nº 306/2003, de 25-06-2003, Proc. 382/2003 [Cons. 28 mai. 2021] Disponível em: <https://dre.pt/web/guest/pesquisa/-/search/671046/details/normal?q=382%2F2003>.

artigos 26º, nº 1 e 18º, nº 2 da Constituição»[150]. Este Acórdão permite-nos corroborar o defendido no título 3.3. deste trabalho, no sentido de que o dever de informação que se impõe aos trabalhadores não constitui justificação para toda e qualquer indagação por parte do empregador e, por isso, aqueles podem legitimamente recusar-se a prestar essas informações.

Já no Acórdão de 5 de julho de 2007[151], o STJ debruçou-se sobre a natureza privada ou laboral dos e-mails trocados entre colegas de trabalho, ao abrigo da proteção conferida pelo art. 21º do CT às mensagens pessoais e à informação não profissional que o trabalhador recebe, consulta ou envia através de correio electrónico. Neste caso, o STJ entendeu que não só as matérias elencadas no art. 16º, nº 2 do CT revestiam *«a natureza de comunicações de índole pessoal, nos termos e para os efeitos do art. 21º do mesmo código»,* justificando que «não é pela simples circunstância de os intervenientes se referirem a aspetos da empresa que a comunicação assume desde logo natureza profissional, bem como não é o facto de os meios informáticos pertencerem ao empregador que afasta a natureza privada da mensagem e legitima este a aceder ao seu conteúdo». Nesse mesmo Acórdão, o STJ esclareceu que o critério para aferir se as mensagens de correio eletrónico têm natureza privada ou profissional deve ser a vontade dos intervenientes. Além disso, no caso não existia qualquer regra a impedir o uso do correio eletrónico da empresa para usos pessoais, conforme previsto no art. 21º, nº 2 do CT, pelo que tal atuação não era passível de sanção disciplinar e, muito menos, de despedimento.

No mesmo sentido se pronunciou já o Tribunal da Relação de Évora[152], ao afirmar que «o meio de prova em causa, utilizado no procedimento disciplinar, é nulo porque viola o direito fundamental de reserva da intimidade da vida privada e a tutela legal e constitucional da confidencialidade da mensagem pessoal», referindo-se a mensagens enviadas pelo trabalhador num grupo privado do *WhatsApp*, que chegaram ao conhecimento da entidade empregadora.

Mais recentemente, também o Tribunal da Relação de Guimarães[153] proferiu decisão sobre a confidencialidade de mensagens pessoais no correio eletrónico dos trabalhadores, estipulando que «são comunicações privadas as mensagens trocadas entre duas trabalhadoras através do messenger do

---

150 Cfr. Maria Regina Gomes Redinha, *Direitos de personalidade...*, p. 5 e 6.

151 Cfr. Ac. do STJ de 05-07-2007, Proc. 07S043 [Cons. 28 mai. 2021] Disponível em: <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/54d3c9f0041a33d58025735900331cc3>

152 Cfr. Ac. do Tribunal da Relação de Évora de 28-03-2019, Proc. 747/18.5T8PTM.E1 [Cons. 28 mai. 2021] Disponível em:

<http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/55801c7296f02f54802583d90052c54c?OpenDocument&Highlight=0,whatsapp>.

153 Cfr. Ac. Tribunal da Relação de Guimarães de 03-12-2020, Processo 3339/19.8T8BCL-A.G1 [Cons. 28 maio 2021] Disponível em:

<http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/9ea2a56f1f40e44c80258654003730 6f?OpenDocument>.

Facebook em contas que são criadas em nome daquelas e destinadas ao envio e receção de mensagens pessoais e não de serviço». Neste Acórdão, o Tribunal fundamentou a sua decisão na diferença evidente que existe entre as comunicações via *messenger* (que se dirigem a um ou vários destinatários específicos, mas escolhidos pelo remetente) e as publicações efetuadas em grupos ou páginas de redes sociais, pois no primeiro caso existem expectativas legítimas de privacidade, pelo que devem ser consideradas mensagens pessoais, inseridas no âmbito de proteção do direito de reserva à vida privada e da confidencialidade da correspondência.

Por fim, importa referir que, apesar de, regra geral, valer o princípio da irrelevância dos atos da vida pessoal do trabalhador para efeitos de despedimento disciplinar com fundamento em justa causa, o certo é que, não raras vezes, a jurisprudência se tem inclinado em sentido diverso, com a justificação de que, em determinadas situações, existe uma relação entre esses atos pessoais e o cumprimento dos deveres que incumbem aos trabalhadores[154]. Por exemplo, a publicação nas redes sociais de mensagens com conteúdos ofensivos ou difamatórios da entidade empregadora ou do seu representante legal, pode consubstanciar uma violação grave dos deveres laborais e, consequentemente, constituir justa causa de despedimento[155] . A título de exemplo, veja-se o Ac. do Tribunal da Relação de Évora, de 30-01-2014[156], onde consta que «constitui grave violação dos deveres laborais de respeito, urbanidade e mesmo de lealdade devidos ao legal representante da sua entidade empregadora e, nessa medida, constitui justa causa de despedimento, a divulgação feita pelo trabalhador, através da rede social "Facebook", de mensagens cujo teor sabia que feriam a honra e o bom nome do legal representante daquela e demais membros da mesa administrativa».

7. CONCLUSÃO

Da elaboração deste estudo ficou patente que o direito à reserva da vida privada, enquanto direito de personalidade que materializa uma vertente da dignidade da pessoa humana, embora não seja muito antigo, sofreu uma evolução conceptual e social ao longo do tempo, motivada sobretudo pelos avanços tecnológicos e pelo surgimento de uma sociedade de informação,

---

154 Esse entendimento foi perfilhado no Acórdão do STJ de 24 de novembro de 2008, Proc. nº 07S3793; no Acórdão do STJ, de 31 de outubro de 1986; no Acórdão do STJ, de 11 de maio de 1994; entre outros. Cfr. Maria Do Rosário Palma Ramalho, *Tutela da personalidade...,* p. 9.

155 Cfr. Maria Do Rosário Palma Ramalho, *Tutela da personalidade...,* p. 9.

156 Cfr. Ac. do Tribunal da Relação de Évora de 30-01-2014, , Processo 8/13.6TTFAR.E1 [Cons. 30 maio 2021] Disponível em:

<http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/70b93024fca4bc1480257de10056fe9c?OpenDocument&Highlight=0,facebook>.

mas também pelo crescente reconhecimento a cada pessoa do poder de autodeterminação sobre as informações que lhe dizem respeito.

Esta evolução que ocorreu no âmbito conceptual e social teve repercussões na legislação e na jurisprudência nacional e internacional, quer no plano civil, quer no âmbito da relação laboral, tendo culminado com a previsão legal do direito à reserva da vida privada no Código do Trabalho português de 2009.

Uma vez que se trata de um direito cujo conteúdo não é estanque, mas antes varia consoante a conformação que o titular faz do próprio, o direito à reserva da vida privada permite inúmeras possibilidades de abordagem e suscita questões muito diversificadas e atuais, sobretudo no mundo digital, que representa uma verdadeira ameaça para o direito à reserva da vida privada. Tanto assim que foi recentemente reconhecido o direito à privacidade em ambiente digital no art. 8º da Carta Portuguesa de Direitos Humanos na Era Digital[157].

Das inúmeras questões que se podem debater a partir deste direito, aquela que, pela sua centralidade, mais interesse nos suscitou foi a da disponibilidade do direito por parte dos trabalhadores através do consentimento, uma vez que, numa relação profundamente inigualitária desde a contratação até à cessação do contrato, poucas serão as vezes em que a vontade manifestada pelos trabalhadores corresponderá à vontade real.

Ora, a disponibilidade do direito à reserva da vida privada por parte dos trabalhadores constitui precisamente uma manifestação de vontade levada a cabo pelo titular do direito que, não podendo renunciar ao mesmo, consente numa violação daquele por parte da entidade empregadora. Porém, atentas as caraterísticas da relação laboral, facilmente se compreende que o consentimento dos trabalhadores, no sentido de facultarem ou permitirem o acesso a informações da sua vida privada, poderá muitas vezes não ser dado de forma consciente e livre, como deveria. Posto isto, a ideia de que, existindo consentimento, fica afastada a hipótese de lesão, já não é tão consensual como outrora. Pelo contrário, reconhece-se hoje que, apesar de os trabalhadores poderem, voluntariamente, limitar o seu direito à reserva da vida privada, essa disponibilidade apenas poderá ser parcial, não podendo verificar-se uma renúncia ao direito.

Ademais, qualquer limitação voluntária ao mesmo deverá ocorrer através de um ato de vontade livre e esclarecido, como é o consentimento prestado com obediência aos requisitos legalmente exigidos, e ainda deverá passar pelo crivo do princípio da proporcionalidade na sua tríplice dimensão (necessidade, adequação e proporcionalidade em sentido estrito).

Por esse motivo, consideramos que, independentemente de haver disponibilidade do direito por parte do titular, deverá fazer-se uma análise casuística das situações que atentam contra a vida privada dos trabalhadores,

---

[157] Cfr. Lei nº 27/2021, de 17 de maio, que aprova a Carta Portuguesa de Direitos Humanos na Era Digital [Cons. 28 mai. 2021] Disponível em: <https://dre.pt/web/guest/home/-/dre/163442504/details/maximized>

sendo ponderados os interesses (legítimos) da entidade empregadora e o direito do trabalhador à reserva da sua vida privada, apenas sendo de admitir uma limitação desse direito quando se verifiquem três requisitos: a existência de um interesse legítimo da entidade empregadora; o consentimento livre e esclarecido do trabalhador; e a limitação do direito ser proporcional aos objetivos pretendidos com a mesma.

Embora a nível juspositivo tenhamos várias normas relativas ao direito à reserva da vida privada e meios de efetivação do mesmo, a verdade é que as principais questões que se têm suscitado relativamente à violação deste direito ocorrem no âmbito digital, sobretudo na perspetiva da proteção de dados pessoais, e não tanto relacionadas com a validade do consentimento. Assim, é de notar que apesar de já existir alguma jurisprudência do TEDH e dos tribunais portugueses relativamente ao direito à reserva da vida privada na relação laboral, a maior parte das decisões reportam-se ao conteúdo do direito ou à violação do mesmo na relação laboral, através de intromissões indevidas das entidades empregadoras na esfera privada dos seus trabalhadores. Porém, até ao momento, não existem decisões conhecidas no que respeita à disponibilidade do direito levada a cabo pelo trabalhador.

8. BIBLIOGRAFIA

Abrantes, José João Nunes, *Contrato de Trabalho e Direitos Fundamentais*, Coimbra Editora, 2005, ISBN 972-32-1330-3

Amado, João Leal

— *Contrato de Trabalho: Noções Básicas*, 2ª ed., Almedina, 2018, ISBN 978-972-40-7438-2

— *Contrato de trabalho e "direito à mentira": uma solução justa?*, in Revista de Legislação e Jurisprudência, Ano 150º, Nº 4028, Gestelegal, Mai/Jun 2021, ISSN 0870-8487

Andrade, José Carlos Vieira De, *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, Reimpressão, Coimbra, Almedina, 1987

Beer, Jeremy De, *Employee Privacy: The Need for Comprehensive Protection*, Saskatchewan Law Review, Vol. 66 (2), 2003. Disponível em: https://www.academia.edu/15579733/Employee_Privacy_The_Need_for_Comprehensive_Protection (Cons. 17.03.2021)

Canotilho, J. J. Gomes; Moreira, Vital, *Constituição da República Portuguesa Anotada, Arts. 1º a 107º*, vol. I, 4ª ed. rev., Coimbra Editora, 2007, ISBN 978-972-32-1462-8

Campos, Diogo Leite De, *Lições de direitos de personalidade*, 2ª ed. (reimp.), Separata do Vol. 66 (1990) do Boletim da Faculdade de Direito da Universidade de Coimbra, 1995

Carvalho, Orlando De, *Teoria Geral do Direito Civil,* coord. Francisco Liberal Fernandes [et. al.] 3ª ed., Coimbra Editora, 2012, ISBN 978-972-32-2017-9

Castro, Catarina Sarmento E, *A proteção de dados pessoais dos trabalhadores,*

— Parte 1, Questões Laborais, Ano IX, nº 19, Coimbra Editora, 2002, ISSN 0872-8267

— Parte 2, Questões Laborais, Ano IX , nº 20, Coimbra Editora, 2002, ISSN 0872-8267

Coelho, Francisco Manuel De Brito Pereira, *A Renúncia Abdicativa no Direito Civil: algumas notas tendentes à definição do seu regime*, Coimbra, Coimbra Editora, 1995, Studia Iuridica 8, ISBN 972-32-0687-0

Cordeiro, António Menezes, *Direito do Trabalho*, vol.I: Direito europeu. Dogmática geral. Direito coletivo, Coimbra, Almedina, 2018, ISBN 978-972-40-7684-3

Craig, John D.R., *Privacy & Employment Law,* Hart Publishing, Oxford and Portland, Oregon, 1999, ISBN 1-84113-059-1

Davidov, Guy

— *Nonwaivability in Labour Law*, Oxford Journal of Legal Studies (forthcoming), 2020 Disponível em: https://www.academia.edu/42344619/Nonwaivability_in_Labour_Law (Cons. 02.04.2021)

— *The Enforcement Crisis in Labour Law and the Fallacy of Voluntarist Solutions*, The International Journal of Comparative Labour Law and Industrial Relations 26, n. 1, Kluwer Law International BV, The Netherlands, 2010, ISSN 0952-617X, Disponível em: https://www.academia.edu/17924292/The_Enforcement_Crisis_in_Labour_Law_And_the_Fallacy_of_Voluntarist_Solutions (Cons. 17.03.2021)

Dray, Guilherme, *An Introduction to Portuguese Employment & Labour Law*, colab. Catarina Granadeiro, Coimbra, Almedina, 2019, ISBN 978-972-40-8108-3

Fernandes, António Monteiro, *Direito do Trabalho*, 19ª ed., Almedina, 2019, ISBN 978-972-40-8076-5

Ferreira, Diogo Figueiredo Perfeito Dias, *Trabalhador, Reserva da Intimidade da Vida Privada e Redes Sociais, nótulas reflexivas sobre um delicado problema juslaboral*. Disponível em: https://portal.oa.pt/media/132093/diogo-figueiredo-perfeito-dias-ferreira.pdf (Cons. 18.03. 2021)

Guimarães, Maria Raquel, *A Conformação da Liberdade Contratual pela Cláusula Geral da Ordem Pública,* in Derecho y Autonomía Privada: Una Visión Comparada e Interdisciplinar, Granada, Editorial Comares, S.L., 2017, ISBN 978-84-9045-521-0

Hendrickx, Frank, *Privacy, data protection and measuring employee performance. The triggers of technology and smart work*, in European Labor Law Journal, 2018, vol. 9 (2). Disponível em: https://journals.sagepub.com/doi/full/10.1177/2031952518781448 (Cons. 17.03.2021)

Martinez, Pedro Romano, *Direito do Trabalho*, 6ª ed., Almedina, 2013, ISBN 978-972-40-5146-8

Mendes, João De Castro, Direito Processual Civil, vol. I, ed. rev. e act., Lisboa, AAFDL Editora, 1987, ISBN 5606939000774

Mercader Uguina, Jesús R., *Derecho del Trabajo: Nuevas tecnologías y sociedad de la información*, Valladolid, editorial Lex Nova, 2002

Mills, Jon L., *Privacy: the lost right*, Oxford University Press, Inc., 2008, ISBN 978-0-19-536735-5

Monereo Pérez, José Luís, *La dignidad del trabajador: dignidad de la persona en el sistema de relaciones laborales*, Murcia, Ediciones Laborum S.L., 2019, ISBN 978-84-17789-25-1

Moreira, Teresa Alexandra Coelho,

— *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo eletrónico do empregador*, Coimbra, Almedina, 2010, ISBN 978-972-40-4208-4

— *Da Esfera Privada do Trabalhador e o Controlo do Empregador*, Studia Iuridica 78, Coimbra Editora, 2004, ISBN 972-32-1228-5

— *Os direitos de personalidade nas relações de trabalho*, in Direito do Trabalho: Relação Individual, João Leal Amado [et. al.], Almedina, 2019, ISBN 978-972-40-8214-1

Pinto, Carlos Alberto Da Mota; Monteiro, António Pinto; e Pinto, Paulo Mota, *Teoria Geral do Direito Civil,* 5ª ed., Coimbra, Gestlegal, 2020, ISBN 978-989-8951-53-3

Pinto, Paulo Mota,

— *Direitos de Personalidade e Direitos Fundamentais: Estudos,* Coimbra, Gestlegal, 2018, ISBN 978-989-54076-3-7

— *O Direito à Reserva Sobre a Intimidade da Vida Privada,* Coimbra, Faculdade de Direito da Universidade de Coimbra, Sep. do Boletim da Faculdade de Direito, vol. 69, 1993

Ramalho, Maria Do Rosário Palma, *Tutela da personalidade e equilíbrio entre interesses dos trabalhadores e dos empregadores no contrato de trabalho. Breves Notas.* Disponível em: https://www.stj.pt/wp-content/uploads/2014/10/prof_maria_rosario_ramalho.pdf (Cons. 18.03. 2021)

Redinha, Maria Regina Gomes,

— *Direitos de personalidade - anotação aos artigos 16º a 21º do Código de Trabalho de 2003*, Trabalho Académico, Faculdade de Direito da Universidade do Porto, 2005 Disponível em: https://repositorioaberto.up.pt/bitstream/10216/18694/2/39941.pdf (Cons. 17.03.2021)

— *Da proteção da personalidade no Código do Trabalho*, in Para Jorge Leite - Escritos Jurídico-Laborais, coord. João Reis [et. al.], vol. I, Coimbra Editora, 2014, p. 819-854, ISBN 978-972-32-2260-9

Redinha, Maria Regina Gomes; Guimarães, Maria Raquel, "O uso do correio eletrónico no local de trabalho - Algumas reflexões", in *Estudos em homenagem ao Professor Doutor Jorge Ribeiro de Faria*, 2003. Disponível em: https://repositorio-aberto.up.pt/bitstream/10216/24325/2/49769.pdf (Cons. 18.03.2021)

Rodríguez-Piñero, Miguel Royo; Todolí, Adrián Signes (Directores), *Vigilancia y Control en el Derecho Trabajo Digital*, Thomson Reuters, Aranzadi, 2020, ISBN 978-84-1346-553-1

Warren, Samuel D. e BRANDEIS, LOUIS, *The Right to Privacy*, Harvard Law Review, vol. 4, no. 5, 15 Dec. 1890). Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf (Cons. 17.03.2021)

Wright, Tom, *Workplace Privacy: A Consultation Paper*, in Information and Privacy Commissioner/Ontario, 1992. Disponível em: https://silo.tips/download/workplace-privacy-a-consultation-paper (Cons. 18.03.2021)

JURISPRUDÊNCIA

Tribunal de Justiça da União Europeia

Acórdão *Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos e Mario Costeja González*, 13 de maio de 2014. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62012CJ0131&from=PT (Cons. 16.05.2021)

Tribunal Europeu dos Direitos do Homem

Acórdão *Barbulescu v. Romania* (Application no. 61496/08) Strasbourg, 5 set. 2017. Disponível em: http://hudoc.echr.coe.int/spa?i=001-177082 (Cons. 27.05.2021)

Acórdão *Sidabras and Others v. Lithuania* (Applications nos. 50421/08 and 56213/08), Strasbourg, 23 set. 2015. Disponível em: http://hudoc.echr.coe.int/eng?i=001-155358 (Cons. 27.05.2021)

Acórdão *López Ribalda and Others v. Spain* (Applications nos. 1874/13 and 8567/13) Strasbourg, 17 out. 2019. Disponível em: http://hudoc.echr.coe.int/spa?i=001-197098 (Cons. 27.05.2021)

Tribunal Constitucional

Acórdão nº 128/92, de 24 de Julho de 1992, disponível em www.dre.pt

Acórdão nº 306/2003, de 25.06.2003, Processo n.º 382/2003, disponível em www.dre.pt

Acórdão nº 413/2011, de 03.11.2011, Processo n.º 20/11, disponível em www.dre.pt

Supremo Tribunal de Justiça

Acórdão de 25-09-2003, Proc. 03B2361. Disponível em: http://www.dgsi.pt/jstj.nsf/0/0e0db401e6e9d5dc80256dea004e8bba?OpenDocument (Cons. 27.05.2021)

Tribunais da Relação

Acórdão do Tribunal da Relação do Porto, de 11-04-2019, Proc. 24733/17.3T8PRT.P1 Disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/d7c7bbf9d0de6091802583fa003bb587?OpenDocument (Cons. 27.05.2021)

Acórdão do Tribunal da Relação de Évora, de 28-03-2019, Proc. 747/18.5T8PTM.E1 Disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/55801c7296f02f54802583d90052c54c?OpenDocument&Highlight=0,whatsapp (Cons. 28.05.2021)

Acórdão do Tribunal da Relação de Évora, de 30-01-2014, Proc. 8/13.6TTFAR.E1. Disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf-005f080b/70b93024fca4bc1480257de10056fe9c?OpenDocument&Highlight=0,facebook (Cons. 30.05.2021)

Acórdão do Tribunal da Relação de Guimarães, de 03-12-2020, Proc. 3339/19.8T8BCL-A.G1
Disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec-004d3832/9ea2a56f1f40e44c80258654003730 6f?OpenDocument (Cons. 28.05.2021)

PROTEÇÃO DE DADOS SENSÍVEIS DO TRABALHADOR: UMA ABORDAGEM SOBRE O STATUS DA VACINAÇÃO NO AMBIENTE LABORAL

Stephanie Goldstein Costa Carvalho

fefagcc@gmail.com

Resumo: O avanço da vacinação contra a Covid-19 causou grande polêmica no contexto laboral em torno da prova de imunização dos empregados ou do simples questionamento acerca da condição ou não de vacinado dos candidatos a emprego ou dos trabalhadores da empresa.

O *status* de vacinação, por ser um dado relativo à saúde, é um dado sensível, pertencente à categoria especial, e, como tal, o seu tratamento está associado a maiores riscos aos direitos e liberdades fundamentais, podendo resultar comportamentos discriminatórios.

Em virtude da particular sensibilidade que o tratamento desses dados envolve, a investigação sobre a condição de imunização de um empregado deverá ser justa e estritamente necessária para um propósito específico e legítimo.

Palavras-chave: RGPD; dados sensíveis; direitos no trabalho; *status* de vacinação; COVID-19.

Abstract: The roll-out of vaccination programmes against Covid-19 caused great controversy in the work context around the immunisation test of employees or the simple question concerning the vaccination status of job applicants or company workers.

Vaccination status is data related to health and as such is classified as sensitive data. Because it belongs in a special category its treatment is associated with potentially greater risks to fundamental rights and freedoms, which may therefore result in discriminatory behavior.

Due to the particular sensitivity that the processing of this data involves, the investigation into the vaccination and or immunisation status of an employee must be fair and be strictly necessary for a specific and legitimate purpose.

Keywords: GDPR; sensitive data; labour rights; vaccination status; COVID-19.

1. INTRODUÇÃO

O presente trabalho abordará o tema dos dados sensíveis do trabalhador, mais especificamente a recolha, pelos empregadores, de dados relativos à saúde, com a exigência de apresentação do certificado de vacinação contra COVID-19[1].

Como é cediço, a temática da proteção de dados assumiu particular relevância no contexto da pandemia, sendo o direito à privacidade e a investigação sobre o *status* da vacinação dos trabalhadores matérias bastante delicadas e que têm provocado um acirrado debate não só nos meios acadêmico e jurídico, mas também na sociedade em geral, cada lado com fortes argumentos pró e contra a possibilidade desse tipo de investigação. É deste debate que o interesse pelo tema se origina.

O objetivo central da pesquisa, inserida nas atividades do projeto do CIJE "It's a wonderful (digital) world: o direito numa sociedade digital e tecnológica", será abordar a temática a partir de uma perspectiva jurídico-constitucional, por meio da qual serão ponderados os direitos e interesses em conflito, bem como fazer uma reflexão de que forma é possível assegurar uma efetiva proteção aos dados pessoais e sensíveis como um direito fundamental do trabalhador.

Esta dissertação será dividida em três partes, seguidas de uma conclusão.

Na primeira delas, faremos uma abordagem geral e conceitual sobre a temática. Inicialmente, trataremos sobre as mudanças provocadas no mundo do trabalho pela revolução digital e tecnológica e o impacto que esta revolução provocou nos direitos fundamentais dos trabalhadores. Em seguida, faremos uma breve exposição acerca da evolução do direito à proteção de

---

[1] "No dia 31 de dezembro de 2019 a Comissão Municipal de Saúde de Wuhan reportou a verificação de 27 casos de pneumonia de etiologia desconhecida, identificando como principal foco de contágio o mercado municipal de Wuhan, tendo reportado a identificação de um novo coronavírus (SARS-COV-2), responsável pela doença respiratória aguda designada COVID-19, vírus introduzido em humanos por transferência de espécie. Os primeiros casos identificados na União Europeia foram comunicados no dia 24 (França) e 28 (Alemanha) de janeiro de 2020, sendo que a 30 de janeiro a Organização Mundial de Saúde declarou a epidemia do novo coronavírus uma emergência de saúde pública internacional (Public Health Emergency of International Concern – PHEIC), a que se seguiu a declaração do estado pandémico global no dia 11 de março de 2020. O enquadramento cronológico do surto de COVID-19 pode ser consultado em European Center for Disease Prevention and Control Cfr. *European Center* for Disease Prevention and Control, 'Event Background COVID-19' (https://www.ecdc.europa.eu/en/novel-coronavirus/event-background-2019)". *Apud* DIAS, Patrícia Cardoso – Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública. *Julgar On-line*. Jan. 2021(tradução da autora). Disponível em: http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/ (22.3.2022).

dados - e sua íntima relação com o direito à privacidade -, apreciaremos o arcabouço normativo que ampara o direito e exporemos os conceitos e princípios relevantes para a aplicação do regime jurídico da proteção de dados. Todos esses tópicos preliminares destinam-se a munir o leitor da base teórica e jurídica necessária para a melhor compreensão da problemática, que será desenvolvida de maneira mais aprofundada nas linhas seguintes.

Na segunda, a nossa atenção voltar-se-á especificamente aos dados pessoais sensíveis, os quais gozam de uma especial regulação no regime jurídico da proteção de dados pelos riscos significativos para os direitos e liberdades fundamentais que o seu tratamento poderá implicar, inclusive no seio da relação laboral, cuja assimetria das posições jurídicas do empregado e empregador realça ainda mais o risco de tratamento desta categoria de dados.

Na terceira parte, nos debruçaremos mais especificamente sobre a categoria especial dos dados relacionados à saúde. Faremos um pequeno recorte na pesquisa para analisar os desafios existentes em torno da exigência da vacinação na relação de emprego, inclusive sob uma perspectiva jurídico-constitucional, com a finalidade de evidenciar a inquietude que gravita em torno do assunto. Finalmente, encerrado o debate acerca da possibilidade da requisição desse tipo de informação, elucidaremos de que maneira deve ser feita a coleta e o processamento de informações sobre a situação vacinal dos empregados à luz do Regulamento Geral sobre a Proteção de Dados (RGPD), como forma de minorar os impactos desse tratamento para a pessoa-trabalhadora.

Feito este introito, passamos a analisar, de forma crítica e detalhada, as questões acima mencionadas.

2. AS MUDANÇAS PROVOCADAS NO MUNDO DO TRABALHO PELA REVOLUÇÃO DIGITAL E TECNOLÓGICA

Os meios de produção utilizados pela sociedade ao longo da história foram determinantes para a proteção jurídico-econômica atribuída a certos bens. O cultivo da terra foi a principal fonte de riqueza da sociedade agrícola; as máquinas a vapor e a eletricidade estiveram no centro do desenvolvimento da sociedade industrial; e os serviços ocuparam posição de destaque no período pós-guerra[2].

No atual estágio evolutivo da sociedade, atrelado ao rápido avanço tecnológico e à globalização, a informação desponta como o bem jurídico mais valioso, sendo responsável por grandes transformações no processo produtivo e nas relações de trabalho. Há uma nova compreensão entre a relação

[2] Bruno Ricardo Bioni – *Proteção de dados pessoais*: a função e os limites do consentimento. 2ª ed. Rio de janeiro. Forense, 2019. p. 3-5.

tempo-espaço[3], sendo as informações transmitidas a uma velocidade nunca antes imaginável. É possível efetuar transferências bancárias por meio de aplicativos digitais, realizar conferências em escala mundial sem sair de casa e até mesmo controlar a produtividade ou o desempenho dos trabalhadores em tempo real e à distância. A tecnologia e o processamento massivo de dados têm assumido, inclusive, importância transcendental na luta contra a crise provocada pelo COVID-19, ao permitir que organizações sanitárias compartilhem dados relativos à saúde com celeridade[4].

Embora sejam inegáveis os benefícios proporcionados pelas tecnologias da informação e comunicação (TIC), elas suscitam diversos desafios no mundo contemporâneo. Questões como segurança da informação são a todo momento postas em causa. Também são cada vez mais frequentes debates envolvendo temas como a "uberização" ou o trabalho em plataformas digitais, a robotização, a utilização de algoritmos, a inteligência artificial, o teletrabalho e os meios de vigilância à distância, que impactam profundamente as formas de organização do trabalho[5].

A ubiquidade da Internet tem ensejado o chamado fenômeno da "datificação", que significa, de maneira sintética, o ato de "datificar" – pôr em dados – praticamente toda a vida de uma pessoa[6]. O termo "datificação", em inglês *datafication*, foi cunhado por Viktor Schönberger-Mayer e Kenneth Cukier, sendo considerado um fenômeno da explosão informacional que consiste em transformar informações aparentemente irrelevantes em dados que podem ser quantificados e revelar um grande valor agregado pela informação sub-

---

3 "Espaço sem distâncias e um tempo sem demoras". Jean-Emmanuel Ray – Qualité de vie et travail de demain. *Droit Social*. Dialnet. Lisboa. ISSN 0012-6438. Nº 2 (2015), p. 147-154.

4 José Luis Domínguez Álvarez – La necesaria protección de las categorías especiales de datos personales. una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19. *Revista de Comunicación y Salud*. Vol. 10, nº 2 (2020), p. 607-624. Disponível em: http://www.revistadecomunicacionysalud.es/index.php/rcys/article/view/240/197 (25.3.2022).

5 "A evolução começou com o trabalho 1.0., do século XIX e da revolução industrial associado ao surgimento da sociedade industrial, o que originou mudanças no modo de produção e na própria organização do trabalho. Depois temos o trabalho 2.0., do século XX, com o surgimento da produção em massa e advento do Estado Social. Há, depois, o trabalho 3.0, a partir da década de 70 do século passado, com a globalização e o surgimento do trabalho no computador e a informática; por último tem-se o trabalho 4.0, relacionado com a digitalização, o trabalho em plataformas, a economia colaborativa, o trabalho integrado, que origina uma mudança de valores e de novos compromissos sociais. Este tipo de trabalho será mais digital, flexível e interconectado". Teresa Coelho Moreira – Algumas questões sobre trabalho 4.0. *4ª Revolução Industrial*. Ano IX, nº 86, Mar. 2020. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/170751/2020_moreira_teresa_questoes_trabalho.pdf?sequence=1 (6.7.2021).

6 Bruno Ricardo Bioni – *Proteção de dados pessoais*: a função e os limites do consentimento. 2ª ed. Rio de janeiro. Forense, 2019. p. 87.

jacente[7]. Cada informação é "datificada", com o objetivo de monitorar, armazenar e identificar padrões de uso, sendo tal informação utilizada para outras finalidades além daquela para a qual fora originariamente coletada.

A captação de informações pessoais dos indivíduos pode resultar na criação de verdadeiros estereótipos ou perfis que influenciam decisivamente a tomada de decisão desses mesmos indivíduos e a sua interação com outras pessoas. Cria-se o risco de doutrinar-se uma pessoa com base em interesses inferidos a partir do processamento dos seus dados, dificultando-lhe o contato com informações diferentes, ocasionais e fortuitas que escapariam dessa catalogação[8].

Revitaliza-se, em última análise, a própria ideia de vigilância, que deixa de estar associada aos rastros que o indivíduo deixa no ambiente virtual ou *on-line* para estar presente em praticamente todas as atividades realizadas no seu cotidiano[9][10], resultando numa intrusão em atividades que, suposta-

---

7 Viktor Mayer-Schönberger; Kenneth Cukier – *Big Data*: A Revolution that Will Transform how We Live, Work, and Think. Boston, New York, 2013. p. 73-97.

8 Bruno Ricardo Bioni – *Proteção de dados pessoais*: a função e os limites do consentimento. 2ª ed. Rio de janeiro: Forense, 2019. p. 91.

9 *Ibid.*, 2019. p. 88.

10 Com vistas a elucidar a forte presença da tecnologia nas interações sociais, cito o seguinte exemplo adaptado: "Taylor Rodriguez prepara-se para uma rápida viagem de negócios. Ela já arrumou a mala na noite anterior da sua partida e a deixou do lado de fora da casa, em frente à porta, para que alguém a apanhasse. Não há preocupação de que ela seja roubada, pois, além das cameras das ruas estarem vigiando-a, cada item da sua mala possui etiquetas de radiofrequência. Eventual ladrão seria rastreado, juntamente com as roupas, e imediatamente detido. Quem vem apanhar a mala é a própria agência de viagens, mas que não necessitou das instruções com relação à data e hora, pois tais informações já haviam sido sincronizadas entre o calendário do smartphone de Taylor e o cadastro dela na agência. Na verdade, todo o itinerário da viagem está na nuvem - cloud computing -, de modo que a bagagem estará esperando por ela em seu hotel, no destino final da sua viagem. No dia seguinte, pela manhã, o chuveiro já está ligado e as torradas estão quase prontas, esperando pela Sra. Rodriguez. Todos os aparelhos da casa estão cronometrados com o itinerário da viagem. Inclusive, a sua geladeira, que já encomendou bacon e ovos ao supermercado, para quando Taylor retornar de viagem. Pouco mais de 30 (trinta) minutos, o táxi já está buzinando em frente à sua porta. O motorista já tem a rota do aeroporto e toca a playlist de músicas favoritas dela; mais uma vez todos os dados estão sendo compartilhados. É só descer do carro, o pagamento já foi realizado via cartão de crédito. Ela se dirige, então, diretamente ao portão de embarque, porque o aeroporto tem reconhecimento facial que faz o controle automatizado do acesso ao saguão. Enquanto Taylor espera para embarcar na aeronave, ela acessa a sua rede social e compartilha con/seus amigos o local para onde está viajando. Ela avança na suatimelmc e curte uma série de posts sobre os protestos que ocorreram na cidade ontem. Ela aproveita o tempo ocioso para convidar seu colega, que está esperando por ela para a reunião de trabalho, para um jantar. A cidade é reconhecida internacionalmente por seus restaurantes de fast food; eles já acordaram que vão sair da dieta. Nesse meio-tempo, já se passaram 30 (trinta) minutos e o seu relógio começa a apitar, ela tem que se movimentar e seguir a sua rotina de alongamentos. Ela não consegue, pois tem que entrar no avião e seguir viagem. O avião pousa. A Sra. Rodriguez chega finalmente ao seu destino e desativa o modo avião ao seu smartphone. Ela começa

mente, até então, tinham cunho privado. Assim é que o compartilhamento de dados em larga escala e a busca por padrões sobre esses dados pode terminar por afetar, de maneira substancial, o exercício de direitos fundamentais protegidos constitucionalmente, como o respeito à vida privada, que será analisado mais adiante, e o livre desenvolvimento da personalidade, que engloba a autonomia individual e a autodeterminação, assegurando a cada um a liberdade de traçar o seu próprio plano de vida[11].

A onipresença do ambiente digital incrementou-se ainda mais nos últimos anos com a necessidade de cumprir regras de confinamento e de distanciamento em prol do combate à pandemia[12], colocando-se ainda mais em evidência as discussões em torno da privacidade e da proteção de dados, nomeadamente no que diz respeito aos aplicativos de rastreamento de dispositivos móveis COVID-19, associado ao processamento de dados sensíveis de saúde[13].

Ao mesmo tempo em que se efetua o processamento de dados em larga escala e se acentuam o controle e a vigilância dos empregadores sobre seus empregados, especialmente nos momentos de crise como o que ora se vivencia, cresce a ameaça aos direitos de personalidade dos cidadãos em geral e dos trabalhadores em específico, que detêm cada vez menos o controlo sobre os próprios dados[14].

---

a receber anúncios de restaurantes de fast food, cujaÏocalização é coincidentemente a cidade onde ela se encontra, bem como de livros sobre ativismo. Ela não tem que se preocupar com a reserva do restaurante, pois seu colega já o fizera, exceto pelo fato de que ela recebeu ofertas com preço superior ao que foi oferecido a ele. O seu relógio, que apitava momentos antes do embarque, já acrescentou mais 01 (um) quilómetro ao seu treino de corrida para amanhã de manhã, por conta da sua indisciplina registrada minutos antes do embarque. Na mesma hora, ela recebe um e-mail da sua seguradora com as novas condições contratuais para renovar seu plano de saúde. O prémio sofreu um aumento fora dos patamares dos anos anteriores, pois, segundo a explicação da corretora, a propensão de ela adquirir algum problema de saúde aumentou". *Ibid.*, 2019. p. 25-26.

11 ACÓRDÃO Nº 288/1998 do Tribunal Constitucional.

12 Mafalda Miranda Barbosa – *Direito (Civil) em tempos de pandemia*. 1ª ed. Coimbra: Gestlegal, 2021. p. 83.

13 Maria Raquel Guimarães; Maria Regina Redinha – A Portuguese approach to privacy in Covid-19 times: through the keyhole. In HONDIUS, Ewoud [et al.]. *Coronavirus and the law in Europe*. Intersentia, 2021. p. 1012.

14 No modelo de negócio "tradicional, consumidores trocam uma quantia pecuniária por um bem de consumo. (...). Ao passo que, sob um novo modelo de negócio, consumidores não pagam em dinheiro pelos bens de consumo, eles cedem seus dados pessoais em troca de publicidade direcionada. (...). A formatação desse modelo de negócio confirma, portanto, a monetização dos dados pessoais, tornando coerente a *equação econômica* da grande gama de produtos e serviços que são 'gratuitamente' disponibilizados na Internet". Bruno Ricardo Bioni – *Proteção de dados pessoais*: a função e os limites do consentimento. 2ª ed. Rio de janeiro: Forense, 2019. p. 25-27.

O permanente monitoramento por parte das empresas[15], a partir da utilização das mais avançadas tecnologias, tem afetado intensamente as relações laborais e, consequentemente, repercutido sobre o exercício dos direitos fundamentais trabalhistas, tornando-se cada vez mais difícil a separação entre a vida privada e a vida profissional[16]. Além desse desvanecimento da noção de privacidade[17], convive-se com a precarização da força de trabalho[18] e com o aumento das taxas de adoecimento físico e mental dos trabalhadores[19] [20].

---

15 "Para além da utilização de câmaras, e de instrumentos de controlo à distância como a instalação em veículos de empresa de tecnologia GPS a simples avaliação das consultas informáticas do trabalhador permite um ganho de conhecimento que se consubstancia em "poder" na relação laboral - com uma amplitude de vulto." Alexandre Sousa Pinheiro – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 728.

Entrou-se numa nova etapa na vigilância e no controle do homem-trabalhador.

16 "New technologies have compounded the problems. Distance from the employer no longer provides any modicum of autonomy for the employee. Car and cellular telephones, as well as various kinds of beepers, allow managers to reach subordinates at home, during the night, or wherever they may be during the weekend. These practices, which are no longer limited to a few jobs in the security business, constitute a real threat to the private life of the employee." Jean-Emmanuel Ray; Jacques Rojot – Worker Privacy in France. *Comparative Labor Law Journal*. Vol. 17, nº 1 (1995), p. 61-74.

17 "A informática entronizou-se como um verdadeiro símbolo da nossa cultura a tal ponto de se denominar a sociedade moderna como sociedade informática ou sociedade da informação e como era da Big Data, que coloca novos desafios à privacidade das pessoas em geral, e dos trabalhadores em especial, parecendo-se dar revalência ao valo económico relacionado com os dados pessoais e não ao seu valor jurídico". A autora prossegue afirmando que "o computador transformou a economia, a sociedade, a cultura e, inclusive, o ser humano". Teresa Coelho Moreira – Dados pessoais: breve análise do art. 28º da Lei nº 58/2019, de 8 de agosto. *Questões Laborais*. Coimbra: Almedina. Ano XXVI, nº 55 (jul./dez. 2019), p. 41-62.

18 "La irrupción de la digitalización en el mundo del trabajo, tanto desde la perspectiva individual como de la colectiva, está provocando un profundo impacto transversal sobre el conjunto de las instituciones reguladoras de las relaciones laborales". Jesús Cruz Villalón – El impacto de la digitalización sobre los derechos fundamentales laborales. In Miguel Rodríguez-Piñero Royo; Adrián Todolí Signes (coords.) – *Vigilância y Control en el Derecho del Trabajo Digital*. Pamplona: Aranzadi–Thomson Reuters, 2020. p. 35.

19 Vitória Nassar Viapiana; Rogério Miranda Gomes; Guilherme Souza Cavalcanti De Albuquerque – Adoecimento psíquico na sociedade contemporânea: notas conceituais a teoria da determinação social do processo saúde-doença. *Saúde e Debate*. Rio de Janeiro. Vol. 42, Nº Especial (Dez. 2018), p. 175-186. Disponível em: https://www.scielo.br/j/sdeb/a/Y36fDqvZL5Js4nnWpXrYpBb/?lang=pt# (10.2.2022).

20 "Hoje se refere por vezes, a expressão *trabalhador-transparente* ou *trabalhador de vidro* que se apresenta numa espécie de *nudez tecnológica,* na medida em que existe uma automatização de dados sobre o trabalhador que, muitas vezes, incide sobre aspectos que fazem parte da sua privacidade e que, por isso, estão protegidos." Teresa Coelho Moreira – Algumas implicações laborais do Regulamento Geral de Proteção de Dados Pessoais no Trabalho 4.0. *Questões Laborais*. Coimbra: Almedina. Nº 51 (2017), p. 13.

Como era de se esperar, o aumento do uso da tecnologia digital durante a pandemia de COVID-19 trouxe à tona a necessidade de ampliar o escopo da privacidade e comprimir os direitos do empregador, especialmente quando o teletrabalho é realizado a partir de casa[21]. A crise tem sido utilizada como mais uma oportunidade para subordinar os trabalhadores individuais, os governos e até sociedades inteiras para responder às demandas mercadológicas do capitalismo global. Os custos de medidas de austeridade, orientadas pela contenção das despesas do Estado, privatização do setor público, aumento dos impostos, diminuição dos salários e liberalização do direito do trabalho, recaem sobre os indivíduos e podem promover, em última instância, a erosão dos direitos sociais e laborais[22].

A redução da complexidade do social à neoliberalização laboral - acompanhada por práticas sociais de muitos empregadores orientadas pela seletividade, dissimulação, simulação e fraude à lei - subverte o carácter protetor do direito do trabalho à parte mais débil no quadro das sociedades capitalistas e provoca um desequilíbrio entre liberdade e igualdade nas relações laborais[23].

A Declaração de Filadélfia adotada, em 10 de maio de 1944, pela Organização Internacional do Trabalho (OIT) assenta o princípio de que "o trabalho não é uma mercadoria" e estabelece a importância do valor do trabalho como mecanismo de redistribuição e promoção da justiça social. Este mesmo princípio é reforçado décadas mais tarde pela OIT na Comissão Mundial sobre o Futuro do Trabalho, oportunidade em que se defendeu que "A gestão de algoritmos, a vigilância e o controlo através de sensores e de outras formas de monitorização, precisa de ser regulado para proteger a dignidade dos trabalhadores. O trabalho não é uma mercadoria; nem é um robô[24].

Casimiro Ferreira alerta para a inversão desse espírito de Filadélfia a que se tem assistido nos dias atuais, ao observar que o direito se tornou mais uma mercadoria a competir no mercado global onde os sistemas jurídicos mais adequados aos objetivos da rentabilidade financeira competem com os restantes fatores de produção[25]. A precarização dos padrões laborais e a redução da qualidade de vida dos trabalhadores são valorados posi-

---

21 Maria Raquel Guimarães; Maria Regina Redinha – A Portuguese approach to privacy in Covid-19 times: through the keyhole. In HONDIUS, Ewoud [et al.]. *Coronavirus and the law in Europe*. Intersentia, 2021. p. 1024.

22 António Casimiro Ferreira – Sociedade da Austeridade e direito do trabalho de exceção. Coimbra: Vida Económica, 2012. p. 12-14.

23 António Casimiro Ferreira – Sociedade da Austeridade e direito do trabalho de exceção. Coimbra: Vida Económica, 2012. p. 87 e 94.

24 Organização Mundial Sobre O Futuro Do Trabalho – Trabalhar para um Futuro Melhor: Comissão Mundial sobre o Futuro do Trabalho. Lisboa: OIT, 2019.

25 António Casimiro Ferreira – *op. cit.*, p. 113.

tivamente como um fator competitivo, provocando, com isso, a degradação do trabalho à escala global[26].

O direito do trabalho protagoniza várias tensões no seio da relação capital x trabalho. Casimiro Ferreira ressalta a importância de uma organização justa do trabalho, alicerçada na presença dos valores éticos do respeito, da dignidade e da autoestima, elementos de uma ética cívica construída sobre a não dissociação entre a organização das sociedades e as suas dimensões normativas."[27].

É, nessa perspectiva, com vistas a evitar que o trabalhador seja reduzido a um puro agente produtivo, submetendo a sua vida inteira, directa ou indirectamente, ao poder diretivo do empregador[28], que assenta a premissa de regulação e efetivação dos direitos sociais, nomeadamente o direito à proteção de dados, como expressão direta da própria personalidade da pessoa-trabalhadora[29].

A rápida evolução tecnológica criou novos desafios a propósito do direito da proteção dos dados pessoais, exigindo um quadro normativo sólido e que seja capaz de gerar a confiança necessária ao desenvolvimento da economia digital do mercado interno[30]. É neste cenário que ganha relevância o estudo do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que tem por objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares[31].

3. A IMPORTÂNCIA DA TUTELA DOS DIREITOS E LIBERDADES FUNDAMENTAIS DOS TRABALHADORES FACE AO AUMENTO DO USO DAS TECNOLOGIAS DA INFORMAÇÃO

Embora a questão da proteção de dados não seja nova, ganhou especial relevância nos últimos anos com a entrada em vigor do Regulamento Geral sobre a Proteção de Dados (UE) 2016/679 (RGPD), que, revogando a Diretiva

---

26 *Ibid.*, p. 129.

27 *Ibid.*, p. 127.

28 Tereza Coelho Moreira – Da Esfera Privada do Trabalhador e Controlo do Empregador. *Studia Iuridica 78*. Boletim da Faculdade de Direito da Universidade de Coimbra, Coimbra Editora, 2004, p. 392.

29 Beatriz De Felipe REIS – *O direito fundamental à proteção de dados pessoais e sensíveis do trabalhador frente às novas tecnologias da informação e comunicação*. Criciúma, 2019. Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade do Extremo Sul Catarinense (UNESC).

30 Considerando 7 do RGPD.

31 Considerando 2 do RGPD.

95/46/CE, tem previsão de aplicação direta nas ordens jurídicas nacionais dos Estados-Membros[32].

A relevância do tema é corroborada pela Declaração do Centenário da OIT, aprovada na 108ª Conferência Internacional do Trabalho, a qual busca assegurar políticas e medidas que garantam a privacidade adequada e a proteção de dados pessoais e respondam a desafios e oportunidades no mundo do trabalho decorrentes da transformação digital do trabalho, incluindo o trabalho em plataformas[33].

Como exposto no tópico anterior, uma das consequências que se observa a partir da globalização e do avanço digital e tecnológico é a ameaça a direitos e liberdades fundamentais, dentre os quais podemos citar a reserva da intimidade da vida privada e o livre desenvolvimento da personalidade. A partir de então, novos e complexos desafios surgem em torno da tutela dos direitos fundamentais.

O Direito do Trabalho foi um dos ramos jurídicos mais afetados pelos influxos tecnológicos, especialmente porque o tratamento de dados é uma consequência quase que natural das relações de trabalho, dado que é essencial a recolha de numerosas informações pelo empregador, tanto para o cumprimento de suas obrigações laborais como para o reconhecimento de direitos aos trabalhadores[34]. Se por um lado é certo que o direito à vida íntima e privada não é um direito absoluto e o trabalhador precisa concordar que haja um certo grau de intrusão e consequentemente necessite compartilhar

---

32 "Ocupam-se da protecção de dados pessoais no nosso ordenamento o art. 35.º da Constituição da República e, entre outras, as Leis n.º 67/98, de 26 de Outubro (Lei da protecção de dados pessoais face à informática); n.º 41/2004, de 18 de Agosto, (Tratamento de dados pessoais e protecção da privacidade no sector das comunicações electrónicas); n.º 12/2005, de 26 de Janeiro, (Informação genética pessoal e informação de saúde); Lei n.º 34/ 2013, de 16 de Maio – (Utilização de sistemas de videovigilância pelos serviços de segurança privada e de autoprotecção). No direito comunitário, esta matéria encontra-se ancorada em várias Directivas, cuja transposição é, de resto, a matriz da legislação ordinária portuguesa: Directiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, (Protecção das pessoas singulares no que respeita ao tratamento de dados pessoais e à livre circulação desses dados); Directiva 2000/31/CE, de 8 de Junho de 2000, (Comércio electrónico); Directiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, (Tratamento de dados pessoais e protecção da privacidade no sector das comunicações electrónicas); e a Directiva 2006/24/CE, de 15 de Março de 2006 (Conservação de dados das comunicações electrónicas e alteração da Directiva 2002/58/CE)". Maria Regina Gomes Redinha – Da Protecção da Personalidade no Código do Trabalho. *Para Jorge Leite*: escritos jurídico-laborais. Coimbra: Coimbra Editora, 2014. p. 826-827.

33 Declaração Do Centenário Da Oit Para O Futuro Do Trabalho: adotada pela Conferência Internacional do Trabalho na sua 108ª sessão. União Geral de Trabalhadores (coord.). Lisboa. UGT, 2019. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-lisbon/documents/publication/wcms_749807.pdf (6.7.2021).

34 Elisa Sierra Hernáiz – *Las categorías especiales de datos del trabajador*: Estudio de los límites y garantías legales para su tratamiento en la relación laboral. Pamplona: Aranzadi–Thomson Reuters, 2021. p. 120.

alguns dados pessoais com o seu empregador, por outro lado o empregador deve observar determinados limites no tratamento desses mesmos dados, sendo óbvio que o nível de intrusão tolerado dependerá muito da natureza do emprego, bem como das circunstâncias específicas que envolvam a relação de emprego[35].

O aumento do uso das tecnologias da informação[36] impulsionou o crescimento de questões relacionadas com a privacidade no ambiente de trabalho[37], intensificando-se, com isso, o enfoque sobre os direitos de personalidade do trabalhador no âmbito da relação laboral ou na chamada "cidadania na empresa"[38], que está associada à ideia de que o trabalhador não perde o direito à individualidade, ou seja, de que não deixa de ser pessoa, só por estar integrado na empresa[39].

A tutela da reserva da intimidade da vida privada aplica-se, nos termos do art. 18, n. 1, da Constituição da República Portuguesa (CRP), às relações entre particulares[40], especialmente àquelas em que exista uma posição de su-

---

35 Grupo de Trabalho de Proteção de Dados do Art. 29. Parecer nº 8/2001, sobre o tratamento de dados pessoais no contexto laboral, adotado em 13 de setembro de 2001, WP 48, p. 19. Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2001/wp48_en.pdf (19.7.2022).

36 Teresa Coelho Moreira – As novas tecnologias de informação e comunicação e o poder de controlo eletrónico do empregador. In *Estudos do Direito do Trabalho*. Coimbra: Almedina, 2011. p. 11-34.

37 Por vezes, esse nosso "Admirável" Mundo Novo do Trabalho mais parece um "Abominável" Mundo Novo do Trabalho. Tereza Coelho Moreira – "Novas Tecnologias: Um Admirável Mundo Novo do Trabalho?". In *Estudos do Direito do Trabalho*. Coimbra: Almedina, 2011. p. 15-52.

38 José João Abrantes – Contrato de Trabalho e Direitos Fundamentais. Coimbra: Coimbra Editora, 2005. p. 59 e ss. *Apud* Sónia Kietzmann Lopes – Direitos fundamentais e direitos de personalidade do trabalhador à luz do Código do Trabalho. In Direitos Fundamentais e de Personalidade do Trabalhador (3ª ed.). *Centro de Estudos Judiciários*. Jun. 2019, p. 25-36. Disponível em http://www.cej.mj.pt/cej/recursos/ebooks/trabalho/eb_DireitoPersonalidade2019.pdf?id=9&username=guest (8.7.2022).

39 "A inclusão dos artigos sobre direitos de personalidade no Código do Trabalho é expressão de uma certa constitucionalização da relação laboral e da noção de que não existe, por um lado, o trabalhador e, por outro, o cidadão, mas antes a pessoa que é simultaneamente cidadão e trabalhador subordinado, referindo-se à "presunção de liberdade", que implica que qualquer restrição aos direitos fundamentais tem que ser justificada, adequada e proporcional face a outro valor que no caso concreto deva ser considerado mais importante". Diogo Coelho; José Miguel Vitorino – Dos Direitos Fundamentais da vida privada do trabalhador e da sua tendencial limitação nas organizações de tendência. *Questões Laborais*. Coimbra: Almedina. Nº 49 (2017), p. 63-64.

40 "Invoca-se, designadamente, a superação de uma perspectiva estritamente liberal – em que os direitos fundamentais como direitos subjetivos públicos visavam defender o indivíduo perante o Estado, só ganhando sentido nas relações com este – e a constatação de que os direitos fundamentais têm como missão proteger a pessoa também contra os poderes existentes no âmbito da sociedade (sendo deste âmbito) que provêm também relevantes ameaças." Sobre a eficácia horizontal dos direitos fundamentais: Paulo Mota

premacia no funcionamento da economia, a começar pelos empregadores no âmbito da relação laboral[41]. Com efeito, os atributos de personalidade do trabalhador são mantidos e reforçados em vista do potencial conflito dentro do contexto de emprego[42].

Além disso, é preciso ter em mente que o respeito pelas liberdades e direitos fundamentais não têm início apenas quando do aperfeiçoamento da relação de trabalho. É, sobretudo, nas fases pré-contratuais, durante o processo de seleção ao emprego, quando o indivíduo está desempregado e, portanto, mais vulnerável, que carece de uma maior proteção.

Em suma, com o avanço das tecnologias da informação e o consequente aumento da circulação dos dados pessoais, inclusive no âmbito das relações laborais, urge a necessidade de reequacionamento dos direitos e liberdades fundamentais, nomeadamente o direito à vida íntima e privada[43], que, por ter sido um dos direitos mais afetados, merecerá uma análise em apartado no tópico seguinte.

4. RELAÇÃO ENTRE O DIREITO À PRIVACIDADE E O DIREITO À PROTEÇÃO DE DADOS

O direito à reserva da intimidade da vida privada, consagrado no art. 26 da CRP, tem sido caracterizado pelo Tribunal Constitucional, à falta de uma definição legal, como "o direito a uma esfera própria inviolável, onde ninguém deve poder penetrar sem autorização do respectivo titular"[44]. Compreende o direito a impedir o acesso de estranhos a informações sobre a vida privada e

Pinto – In *Direitos de Personalidade e Direitos Fundamentais*: Estudos. 2ª ed. Coimbra: Gestlegal, 2018. p. 104-105.

41 "En esa clave, resulta de especial relevância el carácter irrenunciable otorgado a los derechos fundamentales, que presenta especial significación en el âmbito de las relaciones laboralcs, donde bien es conocido el débil juego de la autonomia individual de la voluntad. Ello comporta que la irrenunciabilidad de los derechos fundamentales deba adquirir matices de intensidad superiores a los que con carácter general presenta la irrenunciabilidad de los derechos laborales contemplados en la legislación ordinária". Jesús Cruz Villalón – El impacto de la digitalización sobre los derechos fundamentales laborales. In Miguel Rodríguez-Piñero Royo; Adrián Todolí Signes (coords.) – *Vigilância y control en el Derecho del Trabajo Digital*. Pamplona: Aranzadi–Thomson Reuters, 2020. p. 40.

42 Maria Raquel Guimarães; Maria Regina Redinha – A Portuguese approach to privacy in Covid-19 times: through the keyhole. In Ewoud Hondius [et al.]. *Coronavirus and the law in Europe*. Intersentia, 2021. p. 1018-1019.

43 A tutela da vida privada é, inclusive, reconhecida pelo considerando 4 do RGPD, que dispõe que "O presente regulamento respeita todos os direitos fundamentais e observa as liberdades e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais (...)".

44 Ver acórdãos n.º 355/97, 128/92 e 319/95 do Tribunal Constitucional.

familiar e o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem[45].

Apesar de não ser fácil demarcar a linha divisória entre a vida privada e familiar e o âmbito mais ou menos aberto à publicidade - nomeadamente porque existem inúmeras variantes a serem consideradas, dentre as quais podemos destacar a exposição pública, a atividade profissional e os próprios limites que as pessoas traçam para sua privacidade[46] - a teoria das três esferas[47], caracterizada por distinguir entre as esferas íntima, privada e social, ajuda a compreender os limites deste direito. A esfera íntima corresponde ao "núcleo duro", "irredutível" do direito à reserva da intimidade da vida privada, reconhecido no artigo 26 da Lei Fundamental", insusceptível de ser contrapesado ou limitado "mesmo perante a invocação de um "interesse prevalente da comunidade" ou "interesse público de excepcional relevo"[48]; a esfera privada admite ponderações de proporcionalidade; e a esfera social estaria já no campo do direito à imagem e à palavra e não do direito à intimidade da vida privada[49].

A proteção da intimidade da vida privada assume dimensão relevantíssima no contexto das relações jurídico-laborais, sendo objeto de desenvolvimento no quadro normativo estabelecido pelo Código do Trabalho (CT), que impede, em última medida, intromissões infundadas e excessivas da entidade empregadora sobre a vida privada e familiar dos trabalhadores (art. 16)[50].

Para além do "direito de cada um a ver protegido o espaço interior ou familiar da pessoa ou do seu lar contra intromissões alheias"[51] (vertente negativa), tende hoje a reconhecer-se, igualmente, uma outra dimensão de cariz positivo ou dinâmico, associada ao controle dos indivíduos das informações

---

45 J.J. Gomes Canotilho; Vital Moreira – *Constituição da República Portuguesa Anotada*. Vol. I. 4ª ed. revista. Coimbra: Coimbra Editora, 2007. p. 467.

46 Maria Raquel Guimarães; Maria Regina Redinha – A Portuguese approach to privacy in Covid-19 times: through the keyhole. In Ewoud Hondius [et al.]. *Coronavirus and the law in Europe*. Intersentia, 2021. p. 1012.

47 A chamada "teoria dos círculos de protecção" ou "teoria das esferas" foi difundida por Heinrich Hubman, com o seu "Das Persomlichkeitrecht", de 1953, segundo o qual a preservação jurídica da personalidade contra a "massificação" e a "curiosidade" implica o reconhecimento na pessoa de três "círculos de proteção": "esfera individual", "esfera privada" e "esfera secreta". A primeira respeita ao ser individual integrado no mundo e ao seu valor singular na área pública, ao passo que as esferas "privada" e "secreta" se manifestam através da "proteção contra a área pública". Prossegue o autor afirmando que, apesar das críticas à teoria das esferas, o seu contributo é inegável, na medida em que os seus elementos se mostram ainda hoje como "paradigmas de apreciação da personalidade". Alexandre Sousa Pinheiro – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 447-453.

48 Acórdão 368/02 do Tribunal Constitucional.

49 Rui Medeiros – Anotação ao artigo 64º. In Jorge Miranda; Rui Medeiros – *Constituição Portuguesa Anotada*. Vol. I, 2ª ed. revista. Coimbra: Coimbra Editora, 2010. p. 620.

50 *Ibid.*, p. 623.

51 Acórdão nº 128/92 do Tribunal Constitucional.

que lhe digam respeito, sejam essas informações de caráter íntimo ou não. É a propósito dessa nova dimensão que se depreende o direito à autodeterminação informacional, que nada mais é do que o direito de cada indivíduo dispor de maneira livre dos respectivos dados pessoais e, assim, determinar os termos de acesso e utilização desses mesmos dados[52]. O titular da informação começa a assumir um controle ativo sobre os seus dados, passa a ter o direito de ser informado com exatidão sobre as informações que são coletadas, quem as opera, para quem são transferidas e qual a finalidade do recolhimento.

É diante desse panorama que se impôs a necessidade de redefinição do conceito tradicional de privacidade, para que fosse capaz de assegurar uma proteção mais ampla e eficaz relativamente à circulação das informações pessoais[53], notadamente porque tais informações representam a própria identidade dos indivíduos, são o prolongamento de sua personalidade[54].

4.1. O DIREITO À PROTEÇÃO DE DADOS COMO DIREITO AUTÔNOMO

Em que pese a relação existente entre o direito à privacidade e o direito à proteção de dados, Alexandre Sousa Pinheiro ressalta que "a privacidade e os direitos à protecção e reserva da vida privada não ocupam o espaço próprio do direito à proteção de dados pessoais". Segundo o autor, "a protecção de dados – *Datenschutz*, na terminologia original alemã – está associada a informação existente e conservada – informaticamente ou em ficheiros manuais – sobre o indivíduo e não ao seu desenvolvimento existencial, aos seus comportamentos adoptados enquanto tais ou socialmente projectados"[55].

---

52 Rui Medeiros – *Op. cit.*, p. 620.

53 Andréa Dourado Costa; Ana Virginia Moreira Gomes. Discriminação nas relações de trabalho em virtude da coleta de dados sensíveis. *Scientia Iuris*. Londrina. Vol. 21, nº 2 (Jul. 2017), p. 214-236. DOI: http://dx.doi.org/10.5433/2178-8189.2017v21n2p214. Além disso, como adverte Pinheiro, "O uso precoce do ambiente digital conduz à 'displicência própria da intimidade'. Não se pensa nas consequências da informação deixada no espaço global; o mais habitual consiste, até, em não adquirir consciência do facto de o nome, o endereço de correio electrónico e até a morada serem, na linguagem europeia, 'dados pessoais'. Apenas quando sofre consequências – o caso típico situa-se no campo laboral – da colocação online de fotografias ou atitudes mais deslocadas do comum, o digital native enceta um processo de reflexão que pode conduzir a uma maior prudência futura (o que não apaga os conteúdos extraídos da rede e já armazenados por outros)". Alexandre Sousa Pinheiro – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 239.

54 "Privacy is not a fossilised concept but a dynamic notion that has been developing over decades in a non-linear way, adjusting to contemporary requirements of a complex global digital world." Maria Raquel Guimarães; Maria Regina Redinha – A Portuguese approach to privacy in Covid-19 times: through the keyhole. In Ewoud Hondius [et al.]. *Coronavirus and the law in Europe*. Intersentia, 2021. p. 1010.

55 Alexandre Sousa Pinheiro – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 771.

Com efeito, não há coincidência absoluta entre os dados pessoais e a intimidade ou a vida privada das pessoas. É dizer, nem todos os dados pessoais são dados íntimos ou privados, tampouco a privacidade se restringe aos dados pessoais. Do mesmo modo que há dados que são públicos, há aspectos da vida privada que não constituem e nem se podem traduzir em dados pessoais, como é o caso do recinto doméstico. Para além disso, há dados pessoais que para determinados efeitos são considerados como dados privados e para outros são considerados como dados públicos[56].

Por conseguinte, o direito à reserva sobre a intimidade da privada e o direito à proteção de dados pessoais distinguem-se na sua formulação e alcance, projetando-se a tutela deste último a todas as operações e categorias de dados pessoais tratados independentemente da relação que se estabelece com a privacidade.

O direito à proteção dos dados pessoais não deve ser concebido como uma "mera "evolução do direito à privacidade[57], ele possui uma "relação umbilical e directa" com "integridade informacional"[58], na medida em que estabelece que o tratamento dos dados pessoais não deve afetar o desenvolvimento da personalidade humana[59], porém vai além da visão dicotômica público e privado[60]. Outrossim, embora a tutela dos dados ligados a aspectos da vida íntima do indivíduo deva ser mais intensa, o direito à proteção dos dados pessoais não está circunscrito à zona restrita da intimidade, está, antes, identificado com o direito mais amplo da privacidade, na medida em que está relacionado aos traços identificadores de um sujeito e ao seu comportamento nas relações sociais, está preocupado no desenvolvimento da personalidade do indivíduo sem se expor ao público além do que se entende como conveniente.

---

56 Joaquín García Murcia; Iván Antonio Rodríguez Cardo – Implicaciones laborales del Reglamento 2016/679 de la Unión Europea sobre Protección de datos personales. *Questões Laborais*. Coimbra: Almedina. Ano 24, nº 51 (jul./dez. 2017), p. 36.

57 Bruno Ricardo Bioni – *Proteção de dados pessoais*: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2019. p. 92.

58 Alexandre Sousa Pinheiro – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 771.

59 "A pessoa humana é, pois, objeto de proteção jurídica como centro autónomo de decisão ou, também na expressiva formulação de Orlando de Carvalho, 'raiz de um poder de autodeterminação', conferindo-lhe o direito ao livre desenvolvimento a 'abertura de um espaço livre para 'auto-realização' consciente e conformadora'." Paulo Mota Pinto – In *Direitos de Personalidade e Direitos Fundamentais*: Estudos. 2ª ed. Coimbra: Gestlegal, 2018. p. 27.

60 "Nada é privado nem público em si mesmo mas sim de forma contextualizada [...]. O espaço privado não é simplesmente o que resta quando o espaço público já não está presente, assim como o espaço público não é simplesmente o que resta quando o espaço privado já não está presente. Mesmo no espaço público a vida privada pode estar presente, como por exemplo um casamento, cujo cortejo a caminho da igreja é um ato público." Victor CORREIA – *Sobre a privacidade*. Óbidos: Sinapis, 2016. p. 44-55.

Segundo Alexandre Sousa Pinheiro, enquanto a autodeterminação informacional exprime-se como uma liberdade, a proteção de dados é pensada como uma garantia, o seu fundamento[61]. O direito à proteção de dados reveste a natureza de um direito complexo que integra diferentes posições jurídicas, sendo o direito de acesso e retificação dos dados ou até mesmo da oposição a decisões automatizadas diante de práticas discriminatórias bons exemplos de desdobramentos da sua concepção autónoma no âmbito dos direitos de personalidade[62], que dada a sua importância para a sociedade atual, é concebido, nos dias atuais, como um verdadeiro "petróleo da internet[63]"[64].

O dado pessoal envolve tanto uma informação relativa à vida privada como à vida profissional e social[65]. Ainda de acordo com Alexandre Sousa Pinheiro a distinção entre direito à proteção de dados, privacidade e vida privada manifesta-se a partir do próprio conceito de dado pessoal ("informação que identifica ou torna identificável uma pessoa"), pois, como se pode perceber, a reserva não se restringe apenas àquelas informações sensíveis – cujo âmbito de proteção está ligado à esfera mais pessoal e/ou íntima do titular de dados -, mas se estende a todos os dados individualizáveis[66], isto é, a toda informação que identifica ou torna identificável uma pessoa.

---

61 Alexandre Sousa Pinheiro – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 805.

62 "A dinâmica de proteção dos dados pessoais foge à dicotomia do público e do privado, diferenciando-se substancialmente do direito à privacidade. Propugnar que o direito à proteção os dados pessoais seria uma mera evolução do direito à privacidade é uma construção dogmática falha que dificulta a sua compreensão. (...) Além disso, observa-se que cada vez mais a atividade de tratamento de dados impacta a vida das pessoas, em particular quando elas são submetidas a processos de decisão automatizadas que irão definir seu próprio futuro. Nesse contexto, o direito à proteção de dados pessoais tutela a própria dimensão relacional da pessoa humana, em especial para que tais decisões não ocasionem práticas discriminatórias, o que extrapola e muito o âmbito da tutela do direito à privacidade". Bruno Ricardo Bioni – *Proteção de dados pessoais*: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2019. p. 98-99.

63 Essa frase, originalmente em inglês, "Data is the new oil", foi uma inspiração do matemático londrino, especialista em ciência de dados, Clive Humby. Ela agitou o mundo dos negócios e tornou-se um buzzword, adotado por consultores, executivos e profissionais ligados à transformação digital. Disponível em: https://www.industria40.ind.br/artigo/20949-sim-dados-sao-novo-petroleo#:~:text=Essa%20frase%2C%20originalmente%20em%20ingl%C3%AAs,profissionais%20ligados%20%C3%A0%20transforma%C3%A7%C3%A3o%20digital (14.3.2022).

64 "Estes dados tornaram-se uma nova forma de economia e com um alto valor económico e social". Teresa Coelho Moreira – Dados pessoais: breve análise do art. 28º da Lei nº 58/2019, de 8 de agosto. *Questões Laborais*. Coimbra: Almedina. Ano XXVI, nº 55 (jul./dez. 2019), p. 43.

65 António Barreto Menezes Cordeiro – *Direito da Proteção de Dados à luz do RGPD e da Lei nº 58/2019*. Coimbra: Almedina, 2020. p. 108.

66 Alexandre Sousa Pinheiro – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 772.

É bem certo que os dados pessoais sensíveis que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa, centro da temática do presente trabalho, são considerados uma categoria especial justamente por terem uma ligação intrínseca com a esfera mais íntima e privada do titular, mas, como dito, os dados pessoais não estão reduzidos a esta categoria.

De todo modo, apesar de o direito à proteção de dados se aproximar do direito à privacidade, porém com ele não se confundir, não há como negar que, em se tratando de dados sensíveis, em vista do tipo de informações que integram esta categoria, se avança, em simultâneo, ao domínio do direito à reserva da vida privada.

5. BREVE EVOLUÇÃO HISTÓRICA DA PROTEÇÃO DE DADOS

O Direito da proteção de dados remonta à década de 60 do século passado, a partir do momento em que os avanços tecnológicos passaram a permitir o tratamento automatizado de dados em grande escala, em substituição ao tratamento manual[67].

Nos Estados Unidos da América, a discussão tem início a partir da Constituição, em 1965, do *Special Submmittee on Invasion of Privacy,* que realizou uma série de audiências abordando o assunto e contribuiu de forma substantiva para o caminho legislativo percorrido pelo país a partir da década de 70 do século passado. Porém, até hoje, inexiste, no Direito da proteção de dados estado-unidense, um diploma geral análogo ao RGPD europeu, tendo-se privilegiado uma regulação sectorial[68].

Por sua vez, na Europa, a primeira legislação referente à proteção de dados foi aprovada no ano de 1970, pelo Parlamento do Estado de Hesse, qual seja, o *Hessiches Datenschutzgesetz* (HDSG), que, no entanto, estava circunscrito ao âmbito dos dados recolhidos e tratados por entidades públicas. Apenas em janeiro de 1977 é que foi aprovado o Bundesdatenschutzgesetz (BDSG), a Lei Federal de Proteção de Dados do Estado Alemão que, ao contrário dos diplomas estaduais que lhe precederam, seria aplicável a todos os tratamentos de dados, independentemente da natureza pública ou privada dos responsáveis pelo tratamento. Essa prática de enquadramento geral,

---

67 António Barreto Menezes Cordeiro – *Direito da Proteção de Dados à luz do RGPD e da Lei nº 58/2019*. Coimbra: Almedina, 2020. p. 53.

68 *Ibid*. p. 60-61.

que contrasta com o modelo tradicional estado-unidense, também foi experimentada pela Suécia, com a aprovação, em 1973, do *Datalog*[69].

Na década seguinte, as *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* da OCDE, de 23 de setembro de 1980, e a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, contribuíram de forma decisiva para o processo evolutivo do Direito da proteção de dados, sendo esta última, inclusive, o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados[70], nos termos que mais adiante referiremos a propósito do arcabouço normativo do direito à proteção de dados.

Mas foi só em 1990 que a Comissão apresentou o primeiro projeto legislativo, que culminou, após longas negociações, na Diretriz n.º 95/46/CE, de 24 de outubro de 1995, que, mais tarde, seria revogada pelo então vigente RGPD.

6. ARCABOUÇO NORMATIVO DO DIREITO À PROTEÇÃO DE DADOS

A discussão em torno da temática da proteção das liberdades fundamentais, nomeadamente da vida privada, frente aos perigos do avanço tecnológico, remonta ao final da década de 60 do século passado no âmbito do Conselho da Europa[71].

Diante da conexão existente entre o direito à proteção de dados e o direito à privacidade, o TEDH tem invocado reiteradamente o ar. 8, n. 1, da CEDH, o qual estabelece que "qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência". No entanto, apesar de a jurisprudência do Tribunal de Estraburgo sobre o art. 8 da CEDH extrair a proteção de dados do direito à vida privada e familiar, ela distingue ambos os direitos, na perspectiva que virá a ser reconhecida nos arts. 7 e 8 da CDFUE[72].

Importa destacar que a CEDH foi consagrada antes da utilização generalizada dos computadores, internet e dos assinaláveis progressos tecnológicas, que, como é sabido, aumentaram exponencialmente os riscos relativos ao direito à privacidade e justificaram a autonomização do direito à proteção

---

69 António Barreto Menezes Cordeiro – *Direito da Proteção de Dados à luz do RGPD e da Lei nº 58/2019*. Coimbra: Almedina, 2020. p. 64-66.

70 Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf (18.2.2022).

71 Alexandre Sousa Pinheiro – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 528.

72 *Ibid.*, p. 550.

de dados pessoais, cujo bem jurídico tutelado é a privacidade na sua dimensão de direito à autodeterminação informacional[73].

A Convenção 108 do Conselho da Europa, que, como já mencionado, foi o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados, teve por escopo garantir o respeito pelos direitos e liberdades fundamentais, especialmente o direito à vida privada, em face do tratamento automatizado dos dados de caráter pessoal, conciliando-o com a liberdade de circulação da informação pessoal nos Estados signatários[74].

No âmbito da União Europeia, as bases do Direito da proteção de dados e dos direitos dos titulares de dados estão expressamente positivadas no art. 8 da Carta e no art. 16, n. 1 do Tratado sobre o Funcionamento da União Europeia (TFUE), dispositivos estes que asseguram que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito". Um dos destaques da Carta dos Direitos Fundamentais da União Europeia foi justamente a elevação do conteúdo de proteção de dados ao âmbito do direito primário da União Europeia (art. 8), emancipando-o do direito ao respeito pela vida privada e familiar (art. 7), na perspectiva acima adiantada[75], tendo adquirido expressão de desenvolvimento no artigo 16 do TFUE.

O artigo 16 do TFUE é a base jurídica para o pacote de medidas sobre proteção de dados, adotado em maio de 2016, designadamente do Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que entrou em vigor, simultaneamente, em todos os Estados Membros da União Europeia no dia 25 de maio de 2016[76], sem necessidade de transposição para o direito interno, em atendimento ao desejo de 90% dos europeus de terem o mesmo nível de proteção dos dados pessoais em toda a UE, independentemente do lugar onde os dados são tratados[77].

O art. 1 do RGPD reflete a evolução dogmática em prol da autonomia do direito à proteção de dados, na medida em que, ao contrário do que se ve-

---

73 Disponível em: http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/ (22.3.2022).

74 "Tal como posteriormente na Diretiva nº 95/46/CE (embora em termos distintos), o instrumento convencional mostra a necessidade de harmonizar direitos fundamentais com as vantagens económicas próprias de mercados abertos, onde a livre circulação de dados pessoais constitui um importante factor de gestão". Alexandre Sousa Pinheiro – *Op. cit.*, p. 538.

75 Alexandre Sousa Pinheiro – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 662.

76 Disponivel em: http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/ (22.3.2022).

77 Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt (22.3.2022).

rificava na Diretiva 95/46/CE revogada, não faz qualquer alusão ao direito à vida privada[78].

Para além da infinidade de diplomas relativos ao Direito da proteção de dados no Direito da União[79], o Direito Português também conta com uma multiplicidade de normas que tratam da matéria, seja a nível geral, seja a nível especial.

A CRP reconhece, além do direito fundamental à reserva da intimidade da vida privada, o direito fundamental à proteção dos dados pessoais (cf. art. 26 e 35).

Ela foi pioneira na proteção dos dados pessoais dos cidadãos em relação ao uso das novas tecnologias[80], conferindo ao direito à proteção de dados pessoais dignidade fundamental constitucionalmente autónoma no art. 35[81]. Este dispositivo consagrou o princípio da autodeterminação informativa, que se traduz num conjunto de direitos relacionados com o tratamento automático das informações pessoais dos cidadãos, que visam, simultaneamente, protegê-las perante ameaças de recolha e de divulgação, assim como de outras utilizações possibilitadas pelas novas tecnologias, bem como assegurar aos respetivos titulares um conjunto de poderes de escolha nesse âmbito[82].

---

78 António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 62.

79 Entre os diplomas mais relevante no âmbito do Direito da União Europeia, o autor cita os seguintes: Regulamento (UE) 2018/1807, de 14 de novembro, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia; Regulamento (UE) 2018/1725, de 23 de outubro, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados; Regulamento (UE) n° 611/2013, de 24 de junho, relativo às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretriz 2002/58/CE relativa à privacidade e às comunicações eletrónicas; Diretriz (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho; Diretriz n° 2000/31/CE, de 8 de junho, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrônico, no mercado interno (Diretriz do Comércio Eletrônico); Diretriz n° 2002/58/CE, de 12 de Julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (Diretriz das Comunicações Eletrónicas). *Ibid.*, p. 71-72.

80 "A história contemporânea do Direito português da proteção de dados inicia-se com a Lei n.° 2/73, de 10 de fevereiro195, e o Decreto-Lei n.s 555/73, de 26 de outubro, que instituiu o número nacional de identifícação - o diploma esteve, em grande medida, na origem da inclusão do artigo 35.º no leque dos direitos fundamentais na versão original da CRP." António Barreto Menezes Cordeiro – *Direito da Proteção de Dados à luz do RGPD e da Lei nº 58/2019*. Coimbra: Almedina, 2020. p. 76.

81 Disponível em: http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/ (22.3.2022).

82 Catarina Sarmento e Castro – 40 anos de "utilização da informática": o artigo 35º da Constituição da República Portuguesa. *e-Pública*. Vol. 3, nº 3 (dez. 2016), p. 42-66. Disponível em: https://www.e-publica.pt/volumes/v3n3a04.html (19.7.2022).

No entanto, apesar de o Direito à proteção de dados já estar consagrado na Lei Fundamental desde 1976, o primeiro diploma nacional dedicado exclusivamente à matéria apenas foi aprovado no início da década de 90 do século passado, através da Lei n. 10/91, de 29 de abril, e depois da Lei n. 67/98, de 26 de outubro, que transpôs para a ordem jurídica interna a Diretiva n. 95/46/CE e que foi posteriormente revogada pela Lei n. 58/2019, de 8 de agosto, que tem por objeto assegurar a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679[83].

Finalmente, a preocupação em torno da proteção de dados pessoais e do direito à autodeterminação informacional também aparece no Código do Trabalho, entre os artigos 17 a 22, ao lado de outros direitos de personalidade do trabalhador, como forma de garantir a dignidade da pessoa-trabalhadora.

7. CONCEPTUOLOGIA DO REGIME JURÍDICO DA PROTEÇÃO DE DADOS

Além de trazer novidades no que concerne ao âmbito de aplicação e à exigência de um Encarregado de Proteção de Dados às empresas e instituições que procedam ao tratamento de dados em grande escala e em qualquer caso quando estejam perante o tratamento de dados sensíveis, a revisão e substituição da Diretiva n. 95/46/CE pelo então Regulamento surgiu da necessidade de harmonização dos diversos Direitos nacionais.

O então RGPD oferece definições acerca de conceitos básicos, no seu art. 4, para a melhor compreensão da matéria. O titular dos dados é a pessoa singular a quem se referem os dados pessoais que são objeto de tratamento, enquanto que o responsável pelo tratamento é, nos termos do n. 7 do art. 4 do RGPD, a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais.

Por sua vez, compreende-se por tratamento de dados, a teor do n. 2 do art. 4 do RGPD, uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização,

---

83 "Para além da LE do RGPD, com aplicação tendencialmente transversal, importa considerar a vasta legislação especial em vigor, com destaque para: Lei n.º 59/2019, de 8 de agosto: tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais - transpôs para a ordem jurídica interna a Diretriz (UE) 2016/680, de 27 de abril; Lei n.° 41/2004, de 18 de agosto: proteção de dados pessoais e privacidade nas telecomunicações; Lei n.º 12/2005, de 26 de janeiro: informação genética pessoal e informação de saúde; Lei n.º 26/2016, de 22 de agosto: informação administrativa e ambiental e reutilização dos documentos administrativos; Leis de Videovigilância: Lei n.º 1/2005, de 10 de janeiro; Decreto--Lei n.º 207/2005, de 29 de novembro; Lei nº 51/2006, de 29 de agosto; Lei n.º 33/2007, de 13 de agosto; Lei n.º 34/2013, de 16 de maio." António Barreto Menezes Cordeiro – Op.cit., p. 79.

a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição. Estamos diante de uma noção ampla de tratamento que engloba todo o tipo de operações[84].

Objeto destas operações são os dados pessoais que compreendem, na aceção do art. 4, n. 1, RGPD, qualquer informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»), considerando-se identificável a pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular. Em síntese, os dados pessoais são informações vinculadas, direta ou indiretamente a determinado indivíduo, que revelam algo sobre ele[85].

O Regulamento não dissemina de maneira metódica o conteúdo do direito à proteção de dados pessoais, mas nos socorrendo das suas diretrizes e das orientações jurisprudenciais, temos que esse direito contém dois grandes elementos: o direito a decidir e consentir sobre a obtenção e uso dos dados, e o direito a obter informação verdadeira e pontual acerca do seu tratamento e trajetória[86].

Para além disso, o direito à autodeterminação informativa pode apresentar diferentes facetas. O titular dos dados conta com os direitos de acesso, de retificação, de supressão, de limitação do tratamento, de portabilidade e de oposição (arts. 15 a 21, RGPD), além do direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis (art. 22, RGPD).

O Grupo de Trabalho do art. 29[87], ao analisar a definição de dados pessoais, esclarece que ela assenta em quatro pilares que estão intimamente relacionados e apoiam-se uns nos outros. Em primeiro lugar, "qualquer in-

---

84 Elisa Sierra Hernáiz. *Las categorías especiales de datos del trabajador*: Estudio de los límites y garantías legales para su tratamiento en La relación laboral. Pamplona: Aranzadi–Thomson Reuters, 2021. p. 27.

85 Jessica Andrade Modesto; Marcos ERHADT JÚNIOR – Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pssoais no combate à covid-19. In Rodrigo Nóbrega Farias; Igor De Lucena MASCARENHAS (orgs.) – *COVID-19: saúde, judicialização e pandemia*. Curitiba: Juruá Editora, 2020, p. 149.

86 Joaquín García Murcia; Iván Antonio Rodríguez Cardo – Implicaciones laborales del Reglamento 2016/679 de la Unión Europea sobre Protección de datos personales. *Questões Laborais*. Coimbra: Almedina. Ano 24, nº 51 (jul./dez. 2017), p. 49.

87 Trata-se de um grupo criado pelo artigo 29.º da D 95/46 para aconselhar a Comissão e para contribuir para a aplicação uniforme das normas nacionais que procederam à transposição da D 95/46. O Comité é o sucessor do GT 29, devendo todas as referências normativas consignadas à D 95/46 e ao GT 29 ser entendidas, respectivamente, como remissões para o RGPD e para o Comité. António Barreto Menezes Cordeiro (coord.)

formação"; em segundo lugar, "relativa a"; em terceiro lugar, "identificada ou identificável"; e em quarto lugar, "pessoa singular"[88]. Por prestígio ao poder de síntese do presente trabalho, não nos prolongaremos na análise de cada um desses pilares de forma isolada. Será feita uma análise sucinta e que aborde os aspectos mais relevantes para o estudo que ora se propõe.

O legislador comunitário optou por adotar uma noção ampla do conceito de dado pessoal, que não está circunscrita à esfera dos dados íntimos. Em verdade, abrange todos os aspectos relativos à pessoa, sejam familiares ou sociais, privados ou públicos, físicos ou mentais[89]. A abrangência do conceito pode ser percebida inclusive a partir da diversidade de dados pessoais citados ao longo do RGPD: dados genéticos, dados biométricos, dados relativos à saúde, dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, dados relativos à vida sexual ou orientação sexual de uma pessoa, bem como relacionados com condenações penais e infrações. No contexto laboral, pode-se dizer que qualquer dado relativo ao trabalhador, seja pessoal ou profissional, está compreendido dentro da noção de dado pessoal.

Para que um dado seja considerado como dado pessoal, é preciso que a identificação seja alcançada sem esforços desproporcionados, considerando-se o conjunto de meios que podem ser razoavelmente utilizados pelo responsável do tratamento ou por qualquer pessoa para identificar o titular dos dados[90]. Amparado no considerando 26 do RGPD, que faz referência aos meios suscetíveis de serem razoavelmente utilizados quer pelo responsável pelo tratamento quer por qualquer outra pessoa, o TJUE esclarece que não importa se todas as informações que permitem identificar a pessoa em causa estejam na posse de uma única pessoa[91]. Ademais, não é preciso que a informação veiculada de uma pessoa seja verídica, basta que os dados pessoais proporcionem informação[92].

Sobre o conteúdo dessas informações, adquirem particular relevância os dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma

[et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 487.

88 Disponível em: https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf (18.7.2022).

89 António Barreto Menezes Cordeiro – *Direito da Proteção de Dados à luz do RGPD e da Lei nº 58/2019*. Coimbra: Almedina, 2020. p. 108.

90 Elisa Sierra Hernáiz – *Las categorías especiales de datos del trabajador*: Estudio de los límites y garantías legales para su tratamiento en la relación laboral. Pamplona: Aranzadi–Thomson Reuters, 2021. p. 26.

91 TJUE 19-out.-2016, proc. C-582/14 (Breyer).

92 Elisa Sierra Hernáiz – *Las categorías especiales de datos del trabajador*: Estudio de los límites y garantías legales para su tratamiento en la relación laboral. Pamplona: Aranzadi–Thomson Reuters, 2021. p. 22.

pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa, dados que são, pela sua natureza e segundo os termos do considerando 51, RGPD, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais.

Essa categoria de dados será objeto de aprofundamento mais adiante, mas já adiantamos que esses eles fazem parte de uma categoria especial devido a sua proximidade com a esfera mais íntima e privada do titular dos dados e dos riscos de discriminação e violação de liberdades e direitos fundamentais, cujo tratamento está sujeito a um regime jurídico qualificado ou superior relativamente ao tratamento dos demais dados.

8. PRINCÍPIOS RELATIVOS AO TRATAMENTO DOS DADOS PESSOAIS

Consoante o disposto no art. 5, n. 1, do RGPD, todo e qualquer tratamento de dados pessoais deve atentar aos princípios da licitude, lealdade e transparência, da limitação das finalidades, da minimização dos dados, da exatidão, da limitação da conservação e da integridade e confidencialidade.

O princípio da finalidade constitui princípio norteador da proteção de dados, na medida em que os demais princípios gravitam em torno dele. É dizer, os dados devem ser adequados, pertinentes e limitados em relação à finalidade perseguida; devem ser exatos e atualizados em função da finalidade; só devem ser conservados durante o período necessário para as finalidades para as quais são tratados; e a finalidade pretendida tem de ser legítima, ou seja, deve estar em conformidade com o ordenamento jurídico e respeitar os valores fundamentais[93].

De acordo com o princípio da limitação das finalidades, os dados pessoais apenas poderão ser recolhidos quando houver motivos determinados, explícitos e legítimos, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades. Compreende-se que as finalidades prosseguidas devem ser determinadas antes de iniciado o tratamento, não bastando para o preenchimento deste requisito a utilização de expressões vagas como "melhorar a experiência dos utilizadores", "fins publicitários" ou "segurança cibernética"; explícitas, devendo as finalidades eleitas ser informadas aos interessados; e legítimas, exigindo-se um respeito por todas as disposições legais em concreto aplicáveis[94].

---

[93] Teresa Coelho Moreira – Dados pessoais: breve análise do art. 28º da Lei nº 58/2019, de 8 de agosto. *Questões Laborais*. Coimbra: Almedina. Ano XXVI, nº 55 (jul./dez. 2019), p. 54-55.

[94] António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 104.

O tratamento de dados será lícito se tiver como fundamento uma das alíneas do art. 6, n. 1, ou umas das alíneas do art. 9 ou no art. 10, RGPD - que dizem respeito, respectivamente, ao tratamento de dados sensíveis e a dados relacionados com condenações penais e infrações. Será leal na medida em que o tratamento deve atender ao mesmo tempo aos interesses dos responsáveis pelo tratamento e às expectativas legítimas dos titulares de dados. E será transparente quando todo o conteúdo das informações, durante todo o processo de tratamento, for transmitido aos titulares ou a terceiros[95], ou seja, o titular dos mesmos deve saber como, quando, onde e de que forma o tratamento é feito[96]. Segundo Diogo Pereira Duarte, a informação prestada sobre o tratamento de dados pode, aliás, reconduzir a um maior equilíbrio entre os interesses legítimos do empregador e os direitos fundamentais dos trabalhadores (titulares de dados), consoante estabelecido pelo próprio art. 88, n. 2, RGPD[97].

O princípio da minimização dos dados assumiu contornos mais exigentes no Direito vigente se comparado aos termos da Diretiva 95/46/CE, pois agora utiliza-se a expressão "limitados ao que é necessário" em substituição à locução "não excessivos". Diz-se que este princípio é composto por três elementos: *i)* adequação – impõe que a recolha e os demais tratamentos estejam enquadrados nas finalidades prosseguidas; *ii)* pertinência – exige que as atividades dos responsáveis contribuam para a prossecução das finalidades; e *iii)* limitação – o tratamento apenas será considerado juridicamente aceitável se não houver uma alternativa menos invasiva dos direitos dos titulares[98].

Já o princípio da exatidão apresenta as seguintes dimensões: *i)* proibição de recolha ou o armazenamento de dados incorretos; *ii)* atualização dos dados recolhidos sempre que necessário; e *iii)* dever de apagamento ou retificação dos dados incorretos, à luz das finalidades prosseguidas[99].

Segundo o princípio da limitação da conservação os dados devem ser mantidos durante o tempo estritamente necessário para o cumprimento da finalidade perseguida com o tratamento dos mesmos[100].

Os princípios da integridade e da confidencialidade são uma novidade do Direito vigente e mostram uma preocupação com a segurança dos dados ao estipular a adoção de medidas técnicas e organizativas adequadas[101].

---

95 Ibid,. p. 103-104.

96 Teresa Coelho Moreira – *Op. cit.*, p. 54-55.

97 Diogo Pereira Duarte – In António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 526.

98 António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 105.

99 António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 106.

100 António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 106.

101 *Ibid.*, p. 106.

Em suma, as informações pessoais merecem ser tratadas com respeito ao princípio da boa fé, devem ser recolhidas para finalidade determinadas, não podendo ser posteriormente tratadas de forma incompatível com essas finalidades e devem ser adequadas, pertinentes e não excessivas relativamente às finalidades para que são recolhidas e posteriormente tratadas[102].

Finalmente, consigna o art. 5, n. 2, RGPD, que o responsável pelo tratamento é responsável pelo cumprimento dos princípios acima elencados e tem de poder prová-lo. Esta previsão também é uma novidade trazida pelo legislador europeu e reforça as ideias de *compliance* e *accountability* que permeiam todo o RGPD[103].

O respeito a esse conjunto de princípios – que deve ocorrer para todo e qualquer processamento de dados, seja qual for a base legal de tratamento - está em consonância com a ideia da qualidade de tratamento dos dados pessoais e funciona como importante limite ao poder diretivo do empregador, especialmente quando está-se perante o tratamento de dados sensíveis, pois, como tem-se enfatizado, essa categoria de dados pode implicar riscos significativos de discriminação e de violação para os direitos e liberdades fundamentais, por estarem ligados mais diretamente à esfera mais íntima e privada do titular.

9. OS DADOS PESSOAIS SENSÍVEIS

Como tem-se apontado, o direito à proteção de dados é concebido como o direito a manter o controlo sobre as próprias informações e determinar as modalidades de construção da própria identidade e da vida privada, tendo como objetivo não apenas a privacidade, mas também o livre desenvolvimento da personalidade humana, que somente é alcançado se o indivíduo decide por si mesmo a finalidade e a duração do tratamento de seus dados pessoais[104].

---

102 José João Abrantes – Contrato de Trabalho e Direitos Fundamentais. Coimbra: Coimbra Editora, 2005. p. 59 e ss. *Apud* Sónia Kietzmann Lopes – Direitos fundamentais e direitos de personalidade do trabalhador à luz do Código do Trabalho. In Direitos Fundamentais e de Personalidade do Trabalhador (3ª ed.). *Centro de Estudos Judiciários*. Jun. 2019, p. 34. Disponível em: http://www.cej.mj.pt/cej/recursos/ebooks/trabalho/eb_DireitoPersonalidade2019.pdf?id=9&username=guest.(8.7. 2022).

103 António Barreto Menezes Cordeiro (coord.) [et al.] – *Op. cit.*, p. 106-107.

104 J. C. Álvarez Cortés – "La protección de datos de caráter personal en el ámbito de la relación laboral como derecho fundamental inespecífico: [Art. 18.4 CE y normas concordantes]". In J.L. Monereo Pèrez; F. Vila Tierno; J.C. Álvarez Cortés (Dir.). Derechos laborales fundamentales inespecíficos. Comares: Granada, 2020. p. 328. *Apud* Elisa Sierra Hernáiz – *Las categorías especiales de datos del trabajador*: Estudio de los límites y garantías legales para su tratamiento en la relación laboral. Pamplona: Aranzadi–Thomson Reuters, 2021. p. 318.

A Convenção n. 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, que remonta a 28 de janeiro de 1981, já disciplinava, no seu art. 6, sobre "categorias especiais de dados", porém houve uma evolução, no sentido do seu alargamento, ao longo dos anos[105].

O art. 9 do RGPD estabelece que são dados sensíveis aqueles que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

São merecedores de proteção reforçada, através da previsão de um regime jurídico restritivo aplicável ao seu processamento assim como do empoderamento do titular de dados, por pertencerem à esfera mais pessoal e privada do individuo, vinculada a sua dignidade, e cujo tratamento pode dar lugar a discriminações múltiplas[106]. Por conseguinte, ante os impactos negativos que podem ser gerados na esfera jurídica pessoal do titular, a especial sensibilidade desta categoria de dados pessoais requer uma tutela qualificada.

As particularidades do regime de tratamento dos dados sensíveis encontram-se sobretudo nos fundamentos de licitude previstos no art. 9, n. 2, RGPD, donde se percebe, em confronto com o regime comum do art. 6, RGPD, um agravamento dos requisitos legais para o tratamento dos dados pessoais, justamente em virtude da sua natureza – a maioria dos dados sensíveis corresponde a direitos fundamentais – e aos riscos associados ao seu tratamento, em especial o de discriminação[107].

Na esteira do equilíbrio com outros direitos e liberdades fundamentais (considerando 4, RGPD), em que pese o direito à proteção de dados sensíveis ser um direito autónomo e independente, ele mantém estreita relação com os direitos à proteção da vida privada e familiar e da não discriminação[108]. A interconexão entre esses direitos[109] opera contra possíveis intromis-

---

105 Os dados genéticos, biométricos e orientação sexual não eram considerados dados sensíveis no artigo 8.º/1 da Diretiva de proteção de dados em comparação com o RGPD.

106 Elisa Sierra Hernáiz – *Las categorías especiales de datos del trabajador*: Estudio de los límites y garantías legales para su tratamiento en la relación laboral. Pamplona: Aranzadi–Thomson Reuters, 2021. p. 57.

107 António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 136.

108 António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 136.

109 "El empresario está obligado a adoptar las medidas necesarias para que la recogida, tratamiento y guarda de sus trabajadores se realice de una manera segura y con ello garantizar su inviolabilidad y privacidad para evitar que sean utilizados para sancionar o discriminar de forma encubierta a los trabajadores". J. C. Álvarez Cortés – "La protección de datos de caráter personal en el ámbito de la relación laboral como derecho fundamental inespecífico: [Art. 18.4 CE y normas concordantes]". In J.L. Monereo Pèrez; F. Vila Tierno;

sões empresariais que extrapolem o âmbito do exercício legítimo do poder de organização e direção empresarial ou exigências que excedam o normal exercício da prestação laboral[110].

Enquanto os demais dados pessoais dizem respeito a qualquer informação que permita identificar uma pessoa, a categoria dos dados sensíveis está ligada a situações de riscos de condutas discriminatórias e ataques à dignidade da pessoa humana[111]. Segundo Maria del Mar Crespí Ferriol, enquanto os dados pessoais manifestam aspectos da nossa vida privada, os dados sensíveis revelam os aspectos mais íntimos da pessoa, aqueles absolutamente pessoais e intrínsecos de cada indivíduo, cuja divulgação indevida poderá afetar a sua esfera mais íntima, com todas as consequências que isso comporta[112].

Conquanto a proibição de não discriminação assuma especial relevância neste âmbito, a catalogação dos dados sensíveis também está centrada na natureza de direito fundamental daqueles dados, a situação de vulnerabilidade em que o titular dos dados se encontra (*v.g.* dados relativos à saúde) ou as potenciais consequências prejudiciais que resultem do seu tratamento[113]. O critério subjacente à classificação como sensível do dado pessoal será melhor analisada a propósito do tópico seguinte.

Por seu turno, uma vez autorizado o tratamento dessa categoria de dados, nas situações excepcionais contempladas pelo RGPD ou pela legislação específica dos Estados, é preciso atentar-se, ainda, às medidas adequadas para a proteção dos direitos fundamentais, uma vez que o tratamento desses dados supõe um risco acrescido aos seus titulares. A especial sensibilidade em decorrência do perigo de vulnerar direitos fundamentais e liberdades dos indivíduos enseja a aplicação dos princípios gerais dos dados ordinários e normais reconhecidos no RGPD, porém reforçados mediante o

J.C. Álvarez Cortés (Dir.). Derechos laborales fundamentales inespecíficos. Comares: Granada, 2020. p. 328. *Apud* Elisa Sierra Hernáiz – *Las categorías especiales de datos del trabajador*: Estudio de los límites y garantías legales para su tratamiento en la relación laboral. Pamplona: Aranzadi–Thomson Reuters, 2021.

110 Elisa Sierra Hernáiz – *Las categorías especiales de datos del trabajador*: Estudio de los límites y garantías legales para su tratamiento en la relación laboral. Pamplona: Aranzadi–Thomson Reuters, 2021. p. 66.

111 "O conceito de dignidade da pessoa humana é, assim, elevado a valor fundamental que confere sentido e unidade às disposições constitucionais e, em particular às relativas aos direitos fundamentais. A Constituição Portuguesa, como outras constituições democráticas, incorpora, pois, como valor fundamental a referência à dignidade humana, elemento de unidade valorativa do sistema constitucional." PINTO, Paulo Mota – In *Direitos de Personalidade e Direitos Fundamentais*: Estudos. 2ª ed. Coimbra: Gestlegal, 2018. p. 9.

112 Maria Del Marcrespí FERRIOL – El tratamiento de los datos personales relativos a la salud de los trabajadores. *Revista General de Derecho del Trabajo y de la Seguridad Social*. Nº 52 (2019), p. 257-298. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=6876300 (18.7.2022).

113 António Barreto Menezes Cordeiro – *Direito da Proteção de Dados à luz do RGPD e da Lei nº 58/2019*. Coimbra: Almedina, 2020. p. 133.

estabelecimento de garantias adequadas[114]. A título exemplificativo, podemos mencionar a obrigatoriedade da realização de uma avaliação de impacto sobre a proteção de dados no caso de operações de tratamento em grande escala de categorias especiais de dados (art. 30, n. 5, RGPD).

Feitas tais considerações, partamos para a análise do critério subjacente à delimitação dos dados pessoais como sensíveis, cuja proteção, como visto, se distingue pela sua superioridade em relação àquela que é conferida aos demais dados pessoais.

9.1. O ELENCO DOS DADOS PESSOAIS SENSÍVEIS

O art. 9, n. 1, RGPD, estabelece uma proibição geral no tratamento dos dados[115] que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

A partir deste dispositivo legal, vislumbram-se dois grupos. O primeiro diz respeito aos dados pessoais considerados sensíveis porque *são reveladores* da origem racial ou étnica, das opiniões políticas, das convicções religiosas ou filosóficas, ou da filiação sindical do titular de dados. O contexto assume papel relevante para a recondução à categoria deste primeiro grupo[116]. Já o segundo concerne aos dados genéticos, dados biométricos na medida em que identifiquem uma pessoa de forma inequívoca e dados *relativos* à saúde ou *relativos* à vida sexual ou orientação sexual de uma pessoa. Segundo António Barreto Menezes Cordeiro, "o primeiro grupo respeita a resultados decorrentes do tratamento e o segundo grupo a categorias de dados"[117].

---

114 Maria Del Mar CRESPÍ FERRIOL – *Op. cit.*, p. 257-298. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=6876300 (18.7.2022).

115 A proibição geral de tratamento das categorias especiais de dados deve ser entendida como uma salvaguarda de direitos fundamentais em face do tratamento de dados pessoais, que se traduz na necessidade de preencher um dos fundamentos jurídicos (ou finalidades admissíveis) previstos no nº 2, que nada mais constituem do que ponderações do legislador comunitário em relação a restrições a direitos fundamentais. Alexandre Sousa Pinheiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina, 2018. p. 237.

116 "[...] o estado civil permite identificar a orientação sexual, o mesmo se verificando, por exemplo, com a frequência de um determinado estabelecimento ou com a participação numa manifestação ou num evento de cariz político; o nome e a morada podem igualmente revelar a origem racial ou étnica do seu titular." António Barreto Menezes Cordeiro – *Direito da Proteção de Dados à luz do RGPD e da Lei nº 58/2019*. Coimbra: Almedina, 2020. p. 133-134. No mesmo sentido, vide Dissertação Inês Lopes.

117 António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 133.

Devido à tutela reforçada que se concede à categoria especial de dados, faz-se necessário entender o critério que subjaz a qualificação de um dado como dado sensível. Apesar de o art. 9, n. 1, RGPD, elencar os dados que integram a categoria especial, não traz uma definição do que venham a ser esses dados, tampouco uma justificação para o seu tratamento específico[118]. Limitou-se, apenas, a enumerá-los e estabelecer restrições ao seu tratamento. Caberá, portanto, ao intérprete densificar tal delimitação, a fim de proporcionar uma tutela adequada a essa categoria de dados, de antemão robustecida pelo princípio da proibição geral de processamento de dados sensíveis.

A primeira dificuldade reside na infinidade de informações que revelam a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical do titular de dados. Se entendermos que qualquer informação reveladora desses dados seja considerada sensível, poderíamos chegar ao excesso de tratar algumas informações, mesmo as mais triviais, tais como o nome, a língua e a nacionalidade, como sensíveis e sujeitas à proibição geral de tratamento[119]. Porém, cremos que essa não foi a intenção do legislador europeu. A nosso ver, a extensão da categoria dos dados sensíveis a esse ponto pode ser fonte de grave insegurança jurídica, pois, com o avanço da tecnologia e da possibilidade de cruzamento de informações, passariam a ser considerados como dados sensíveis desde os dados mais anódinos, o que minaria, em última instância, o próprio espírito do RGPD, que é também proporcionar a livre circulação dos dados.

A imprecisão da redação do art. 9, n. 1, RGPD, pode ser percebida a partir da referência do Grupo de Trabalho do Art. 29º à criação de dados de categorias especiais por inferência, ou seja, a partir de dados que não sejam dados de categorias especiais *per se*, mas que passem a sê-lo quando combinados com outros dados. Como exemplo cita a inferência do estado de saúde de uma pessoa a partir de registos das suas compras de produtos alimentares, associados com dados relativos à qualidade e ao valor energético dos alimentos[120].

Alexandre Sousa Pinheiro também alerta para o fato de que um conjunto de dados não sensíveis devidamente organizado e tratado pode implicar resultados mais intrusivos do que propriamente o tratamento de dados classificados como sensíveis. Segundo o autor, a classificação dos dados

---

118 Elisa Sierra Hernáiz – *Las categorías especiales de datos del trabajador*: Estudio de los límites y garantías legales para su tratamiento en la relación laboral. Pamplona: Aranzadi–Thomson Reuters, 2021. p. 53.

119 Inês Maria Oliveira Gomes Camarinha Lopes – *O RGPD e a proteção dos dados sensíveis dos menores.* Porto: 17 Dez. 2020. Dissertação de mestrado apresentada à Faculdade de Direito da Universidade do Porto. p. 8.

120 "Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679" do Grupo de Trabalho do Artigo 29º de 6 de fevereiro de 2018, p. 16-17.

como sensíveis pode ser ilusória[121], na medida em que a possibilidade de cruzar ou de proceder a interconexões, na era do *big data*, pode tornar uma informação de caráter aparentemente "bagatelar" num elemento potencialmente sensível[122].

Considerações como as que foram expostas acima podem resultar, como dissemos, num alargamento excessivo na qualificação dos dados sensíveis, ao incluir nessa categoria especial desde as informações mais correntes e que apenas com grande esforço e dependendo das tecnologias empregadas possam revelar informações sensíveis. Entendemos que não basta um indício ou um reduzido grau de probabilidade, deduzido a partir de informação que revele a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, para que um dado seja qualificado como sensível. É preciso analisar, no caso em concreto, a eficácia real do tratamento destes dados na identificação de um dado sensível[123]. A consideração em abstrato de que informações triviais ou do quotidiano possam revelar a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical do titular de dados pode resvalar em conclusões inverídicas sobre o titular e gerar dados pessoais inexatos[124].

O considerando 51, RGPD, pode funcionar como baliza interpretativa para a imprecisão contida na redação da norma do art. 9, n. 1, RGPD, no que concerne aos dados pessoais considerados sensíveis que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical do titular de dados, ao estabelecer que "merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais".

Ora, diversamente do que sucede a partir da leitura isolada do art. 9, n. 1, RGPD, que, como visto, permite uma interpretação muito ampla e imprecisa dos dados pessoais considerados sensíveis que revelem aquelas características, o considerando 51, RGPD, se mostra mais restrito quanto ao critério que subjaz aquela qualificação, ao exigir que se trate de dados "que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos

---

121 Alexandre Sousa Pinheiro – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 648.

122 Maria Eduarda Gonçalves. A Protecção de dados Pessoais em Direito Internacional e em Direito Interno. RMP. Ano 10, nº 40 (1989), p. 19 *Apud* PINHEIRO, Alexandre Sousa – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 642.

123 António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 134.

124 Inês Maria Oliveira Gomes Camarinha Lopes – *O RGPD e a proteção dos dados sensíveis dos menores*. Porto: 17 Dez. 2020. Dissertação de mestrado apresentada à Faculdade de Direito da Universidade do Porto. p. 8.

e liberdades fundamentais". Daí também se compreende que nem todos as informações que contendem com direitos e liberdades fundamentais devem ser consideradas sensíveis, mas apenas aquelas que sejam, pela sua natureza ou na sua essência, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, estando excluídas, portanto, aquelas informações triviais ou quotidianas que apenas em resultado de deduções sobre as mesmas e com bastante esforço possam revelar algum dado mais sensível do titular. Assim sendo, no nosso entendimento, os registos de compras de produtos alimentares não devem ser considerados dados sensíveis, mesmo que, associados a outras informações, sejam capazes de revelar o estado de saúde do indivíduo. Do mesmo modo, apesar de o género ou a idade do titular de dados consistirem em dados pessoais que comportam um risco para o direito fundamental à não discriminação (art. 26 da CRP e art. 21 da CDFUE), tais dados também não devem ser considerados informações particularmente sensíveis, antes pelo contrário, mostram-se triviais[125].

Outrossim, apesar de muitas vezes haver confusão entre a qualificação de um dado como sensível e o risco de discriminação que ele comporta, há de ter em mente que o suposto risco de discriminação do titular de dados não deve ser fator decisivo para a qualificação de um dado como sensível, sob pena de incorrer-se no mesmo excesso que se tem alertado a partir da leitura isolada do art. 9, n. 1, RGPD, para o qual bastaria que os dados pessoais "revelem" a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical[126]. Da mesma forma que uma informação que contende com um direito ou liberdade fundamental não será necessariamente sensível, também não poderá ser enquadrada como tal pelo simples fato de possuir potencial discriminatório. Desse modo, mesmo que se possa inferir, por exemplo, a origem racial do titular dos dados, a partir do conhecimento do seu nome, da sua residência e da sua condição social, e que tal possa resultar em prática discriminatória, o processamento daqueles dados permanecerá acobertado pelo regime dos dados não sensíveis.

Ainda no que concerne aos dados reveladores da origem racial ou étnica, das opiniões políticas, das convicções religiosas ou filosóficas, ou da filiação sindical do titular de dados, importa, também, ter em conta o contexto no qual os dados são tratados. Se indiretamente o responsável pelo tratamento obtém informações que, no contexto da finalidade em que são tratadas, são particularmente associadas às descritas categorias de dados pessoais sensíveis, então será aplicável o regime da proibição geral do art. 9, n.

---

125 Inês Maria Oliveira Gomes Camarinha Lopes – *O RGPD e a proteção dos dados sensíveis dos menores*. Porto: 17 Dez. 2020. Dissertação de mestrado apresentada à Faculdade de Direito da Universidade do Porto. p. 12.

126 *Ibid.*, p. 15.

1, RGPD.[127]. Segundo esta linha de raciocínio, se o conhecimento da origem racial ou étnica, das opiniões políticas, das convicções religiosas ou filosóficas, ou da filiação sindical do titular de dados ocorrer num contexto associado às descritas categorias de dados pessoais sensíveis, então o dado será considerado sensível; em diferentes contextos (*v.g.* conhecimento da cor da pele do consumidor para a venda de produtos de maquilhagem), o dado não será qualificado como tal, pois, neste caso, o que está subjacente é a venda de um bem.

De outra parte, se por um lado pode-se dizer que o art. 9, n. 1, RGPD, peca pelo excesso, também pode-se afirmar que o dispositivo peca por defeito, pois deixa de fora de sua previsão informações que apresentam um grande risco para os direitos e liberdades fundamentais (*v.g.* geolocalização, informações que revelam o histórico criminal de uma pessoa[128] ou o vínculo de filiação de uma criança)[129].

Deve-se avaliar se o dado tratado é sensível do ponto de vista material, ou seja, se o dado, pela sua natureza, é especialmente sensível do ponto de vista dos direitos e liberdades fundamentais, dentro do contexto em que foi coletado. Outrossim, é precipitado dizer que um dado não deve ser considerado sensível só porque não está inserido no elenco formal do dispositivo do art. 9, RGPD, sob pena deixar desamparadas claras situações de discriminação[130].

No tocante ao segundo grupo de dados pessoais sensíveis, a saber, aquelas informações que são relativas à saúde, à vida sexual ou orientação sexual de uma pessoa, o critério subjacente é mais direto, não sendo necessário recorrer-se ao considerando 51, RGPD. Neste caso, para que sejam consideradas sensíveis, bastará, de modo objetivo, que as informações sejam relativas à saúde, orientação sexual ou vida sexual do titular de dados[131].

9.2. A TUTELA DOS DADOS ESPECIALMENTE SENSÍVEIS DOS TRABALHADORES

O direito à proteção de dados é um direito autónomo que visa controlar o fluxo de informações que digam respeito a uma determinada pessoa,

---

127 Inês Maria Oliveira Gomes Camarinha Lopes – *O RGPD e a proteção dos dados sensíveis dos menores*. Porto: 17 Dez. 2020. Dissertação de mestrado apresentada à Faculdade de Direito da Universidade do Porto. p. 13.

128 Os dados relativos à prática de crimes não são considerados dados pertencentes à "categoria especial", todavia pertencem a um regime distinto dos dados não sensíveis, previsto no art. 10º do RGPD.

129 Inês Maria Oliveira Gomes Camarinha Lopes – *O RGPD e a proteção dos dados sensíveis dos menores*. Porto: 17 Dez. 2020. Dissertação de mestrado apresentada à Faculdade de Direito da Universidade do Porto. p. 9-10.

130 António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 88.

131 Inês Maria Oliveira Gomes Camarinha Lopes – *O RGPD e a proteção dos dados sensíveis dos menores*. Porto: 17 Dez. 2020. Dissertação de mestrado apresentada à Faculdade de Direito da Universidade do Porto. p. 8.

relacionadas ou não ao âmbito mais estrito de sua intimidade, para assim preservar o pleno exercício de seus direitos e evitar que a informatização de seus dados pessoais implique comportamentos discriminatórios[132].

Paralelamente ao avanço dos instrumentos tecnológicos, que oferecem a possibilidade de reunir e de cruzar informações, propiciando o acesso aos nossos mais íntimos segredos, incluindo a descoberta de riscos de doenças, escolhas reprodutivas e informações que dizem respeito às nossas relações mais pessoais, verifica-se uma ingerência cada vez maior das empresas na vida privada dos seus funcionários[133].

Ao mesmo tempo em que as ferramentas tecnológicas podem trazer vantagens competitivas para o empresário, se utilizadas inadequadamente, elas também podem ser responsáveis por provocar sérias ameaças aos direitos de personalidade do trabalhador e culminar em atos ilícitos de ordem discriminatória inclusive no âmbito extra-laboral, especialmente quando desembocam na esfera dos dados sensíveis[134].

Como já fora advertido, o ordenamento jurídico trabalhista constitui um dos campos específicos de aplicação do RGPD, uma vez que incumbe ao empregador, para a correta execução do contrato de trabalho, conhecer e tratar uma infinidade de dados pessoais de seus empregados (*v.g.,* acompanhamento da produtividade e do estado de saúde do empregado). Na realidade, antes mesmo de o contrato ser firmado, no decorrer do processo de seleção para o emprego, já são realizadas uma série de operações sobre os dados pessoais dos candidatos à vaga (*v.g.,* através da análise do currículo, dos dados de saúde, do registro criminal e da investigação das redes sociais).

Diante da importância que o tratamento de dados pessoais assume no contexto laboral, o RGPD possui previsão específica, no art. 88, no sentido de que os Estados-Membros possam estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, bem como para efeitos de cessação da relação de trabalho[135].

---

132 Elisa Sierra Hernáiz. *Las categorías especiales de datos del trabajador*: Estudio de los límites y garantías legales para su tratamiento en la relación laboral. Pamplona: Aranzadi–Thomson Reuters, 2021. p. 102.

133 Bradley A. Areheart, Jessica L – Gina Roberts, Big Data, and the Future of Employee Privacy. *The Yale Law Journal*. Vol. 128, nº 3 (2019), p. 710-791. Disponível em: https://www.yalelawjournal.org/pdf/AreheartRoberts_a2gvpzai.pdf (19.7.2022).

134 Andréa Dourado Costa; Ana Virginia Moreira Gomes. Discriminação nas relações de trabalho em virtude da coleta de dados sensíveis. *Scientia Iuris*. Londrina. Vol. 21, nº 2 (Jul. 2017), p. 214-236. DOI: http://dx.doi.org/10.5433/2178-8189.2017v21n2p214.

135 "A diversidade de setores e ramos de atividade gera necessidades distintas de tratamento de dados, no que tange à quantidade de dados, à extensão do tratamento, ao fun-

Em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, como no caso das relações laborais, justifica-se uma proteção jurídica ainda mais reforçada do ponto de vista do tratamento dos dados, sobretudo se esse tratamento envolver informações pertencentes à categoria dos dados sensíveis.

Nesta senda, considerando-se que os dados sensíveis merecem uma proteção específica, por serem especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais e o seu tratamento poder implicar riscos significativos para o direito à reserva da vida privada, o legislador comunitário consagrou, como regra geral, a proibição para o seu processamento (art. 9, n. 1, RGPD), a menos que se verifique um dos casos de derrogação previstos no art. 9, n. 2, RGPD[136], dentre os quais, pela conexão direta com o contexto laboral, destaco as seguintes: o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral" (letra "*b*") ou se "o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico" (letra "*h*").

Todo e qualquer tratamento de dados pessoais, o que, obviamente, inclui os dados sensíveis inseridos no contexto laboral, deve observar os princípios gerais de proteção de dados, os quais correspondem ao elemento vital de proteção que o Regulamento confere aos trabalhadores em relação ao tratamento dos seus dados pessoais[137].

O acesso às informações sensíveis deverá ser realizado da maneira mais objetiva e menos invasiva possível, sendo o tratamento limitado aos casos diretamente relacionados ao cumprimento das obrigações empresariais ou ao exercício dos direitos das pessoas trabalhadoras[138].

---

damento jurídico, ou ao prazo de conservação. Destarte, as atividades que pressuponham tratamento de dados pessoais, e em particular de dados sensíveis, deveriam regulamentar o tratamento de dados, nomeadamente em sede de instrumento de regulamentação coletiva". Alexandre Sousa Pinheiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina, 2018. p. 665.

136 "As exceções à proibição do tratamento de dados pessoais constituem-se estruturalmente como causas de exclusão da ilicitude, no sentido em que um tratamento de dados que, em princípio, seria ilícito cede perante a preponderância de um interesse proporcionalmente mais relevante, que justifica o tratamento". Alexandre Sousa Pinheiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina, 2018. p. 238.

137 Os dados pessoais mantidos por um empregador podem, por exemplo, ser excessivos, mesmo que tenham sido fornecidos voluntariamente por um trabalhador que tenha dado consentimento para sua detenção. De acordo com o Parecer nº 8/2001, sobre o tratamento de dados pessoais no contexto laboral, adotado em 13 de setembro de 2001, WP 48, p. 18. Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2001/wp48_en.pdf (19.7.2022).

138 Elisa Sierra Hernáiz. *Las categorías especiales de datos del trabajador*: Estudio de los límites y garantías legales para su tratamiento en la relación laboral. Pamplona: Aranzadi–Thomson Reuters, 2021. p. 80.

Neste ponto, importa notar que nem todos os dados sensíveis possuem a mesma relevância no contexto laboral, porquanto alguns possuem uma incidência mais direta e necessária (*v.g.*, dados que revelam filiação sindical, dados biométricos ou relativos à saúde) do que outros (*v.g.*, dados que revelam a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou dados relativos à vida sexual ou orientação sexual de uma pessoa)[139]. Assim, ressalvadas algumas situações muito específicas, a exemplo do que acontece em empresas de tendência[140][141], pode-se dizer que, *a priori*, não haverá um interesse legítimo em relação ao tratamento desses últimos dados no contexto laboral. Com efeito, fatos da vida privada que não apresentam qualquer conexão com a vida profissional nem são capazes de destruir a confiança recíproca ou a boa-fé contratual não devem ser relevados para o cumprimento da prestação. O poder directivo do empregador, que se destina a assegurar o bom funcionamento do empreendimento, possui limites resultantes dos direitos e liberdades fundamentais da pessoa- trabalhadora, apenas assumindo relevância aqueles comportamentos extralaborais do trabalhador que incidam directamente sobre a sua aptidão profissional[142].

Como bem adverte Alexandre Sousa Pinheiro, o grau de "intimidade" da informação deve levar em consideração o princípio da finalidade, ou seja, o motivo que justifica o tratamento dos dados[143], de modo que, para que o tratamento dos dados pessoais seja considerado legítimo, deve-se atentar para o princípio da proporcionalidade e verificar se há conexão entre a informação objeto de tratamento e a finalidade para a qual a informação é recolhida.

Em suma, para além das objeções gerais ao tratamento de dados, há de serem adotadas especiais cautelas quando se tem em mira o processamento de dados pessoais dos trabalhadores, sobretudo se eles pertencerem à categoria especial, pois, como temos insistido, os dados enquadrados nesta

---

139 *Ibid.*, p. 87.

140 Ainda que não haja qualquer preceito no ordenamento jurídico português que defina precisamente o que é uma empresa de tendência, deve ser considerada como tal aquela que tenha como característica o desenvolvimento de uma atividade em que a fidelidade a certos princípios ideológicos (inspirados em ideias externa e claramente reconhecíveis) ou religiosos possuem um papel fundamental. Raquel Tavares Reis – *Liberdade de Consciência e de Religião e Contrato de Trabalho do Trabalhador de Tendênci***a**: que equilíbrio do ponto de vista das relações individuais do trabalho? Coimbra: Coimbra Editora, 2004. p. 171-175.

141 "In a decision of 20 November 1986, a case concerning a professor of Protestant Theology who had changed her religious affiliation, the Supreme Court ruled that "section 122-45 is not applicable when the employee, having been hired for a task which ecessitates that she be in harmony of thought and faith with her employer, disregards the obligations born of this commitment.". Exemplos citados pelos autores: Jean-Emmanuel Ray; Jacques Rojot – Worker Privacy in France. *Comparative Labor aw Journal*. Vol. 17, nº 1 (1995), p. 61-74.

142 Diogo Coelho; José Miguel Vitorino – Dos direitos fundamentais da vida privada do trabalhador e da sua tendencial limitação nas organizações de tendência. *Questões Laborais*. Coimbra: Almedina. Nº 49 (2017), p. 60.

143 Alexandre Sousa Pinheiro – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 805.

categoria são merecedores de uma proteção superior ou qualificada relativamente ao tratamento dos demais dados pessoais.

10. OS LIMITES DA INDISPONIBILIDADE NO CONTEXTO LABORAL

Ante a existência da desigualdade de poder entre as partes no contrato de trabalho e a irrefutável superioridade do poder de barganha do empregador, o consentimento assume contornos problemáticos nesse tipo de contrato. Existe a suspeita de que quando um empregado renuncia a um direito trabalhista, essa renúncia não é fruto de uma escolha verdadeiramente livre, especialmente porque a legislação trabalhista foi pensada para proteger a parte mais fraca, no caso o empregado. Como diria Marx, "the appearance of independence is maintained [...] by the legal fiction of a contract"[144]. A liberdade de consentimento não passa, portanto, de uma mera ficção no mundo jurídico.

O contrato de trabalho configura situação ambivalente, pois ao mesmo tempo em que não é possível falar de absoluta liberdade (*v.g.* comprar um sorvete e *business-to-business* em mercados competitivos), na maioria dos casos também não será possível dizer que há completa coerção (*v.g.* uma arma apontada para a cabeça). E, mesmo dentro da categoria dos contratos de trabalho, há inúmeras variáveis que merecem ser ponderadas quando da análise da liberdade do consentimento (*v.g.* se o empregado é qualificado ou não, se recebe altos ou baixos salários, etc)[145].

Segundo Davidov pode-se até supor que há uma certa liberdade quando é feito um acordo que vai além do mínimo legal, mas, mesmo nestes casos, a subordinação continua presente, e mesmo que o empregado tenha uma forte segurança no trabalho que o permita negar algo proposto pelo empregador sem medo de ser demitido, há outros elementos que vão pesar na sua decisão e assim farão com que ela não seja totalmente livre (*v.g.* aspiração de uma promoção no trabalho)[146].

Davidov defende que a previsão de um mínimo não renunciável não prejudica a autonomia do empregado, mas, antes, a assegura, na medida em que a regulação trabalhista tem por objetivo fortalecer a dignidade e a liberdade substancial dos trabalhadores, impedindo-os de fazerem escolhas sob a ameaça de coerção. Segundo o autor, essa intervenção paternalista se justifica para fazer frente a situações em que uma pessoa concorda em

---

144 Karl Marx – *O Capital*: Vol: 1. Editora Nova Cultural, [(1867:197)1996], p. 719.

145 Guy Davidov – 7º Encontro Ibérico Transformações Recentes. Disponível em: https://www.youtube.com/watch?v=0Y8b0o7TLPA&t=8288s (9.5.2022). Vide também Guy Davidov – Non-waivability in Labour Law. *Oxford Journal of Legal Studies*. Vol. 40, nº 3 (2020), p. 482–507. DOI: https://doi.org/10.1093/ojls/gqaa016.

146 Guy Davidov – *Op. cit.* Disponível em: https://www.youtube.com/watch?v=0Y8b0o7TLPA&t=8288s.

limitar sua própria liberdade ou o seu bem estar (*v.g.*, caso de um trabalhador que concorda em submeter-se à possibilidade de dispensas arbitrárias ou discriminatórias em ordenamentos que proíbem esse tipo de dispensa), quando se está perante escolhas baseadas em informações incompletas ou baseadas na confiança e segurança inerentes ao contrato de trabalho, ou quando há um risco de dano para familiares, outros funcionários ou até mesmo para a sociedade em geral (*v.g.*, caso se permita que um funcionário aceite trabalhar recebendo menos do que um salário mínimo, essa sua decisão individual causará um impacto direto sobre todos os demais funcionários, que passarão a ser pressionados, direta ou indiretamente, a também renunciarem de seus direitos trabalhistas). Para o autor, parte do problema pode ser solucionado por meio da criação de um mínimo não renunciável[147].

Porém, de acordo com os ensinamentos do mesmo autor, essa solução não é suficiente, pois em determinadas circunstâncias o consentimento importa e não será possível identificar uma completa coerção. Assim, Davidov propõe uma abordagem alternativa, que parte do princípio de que se não forem observadas determinadas condições ou regras haverá mais chances de que o consentimento dado naqueles moldes não foi válido. Ele divide essas condições em regras procedimentais (projetadas para suportar o consentimento livre e informado tanto quanto possível) e regras substantivas (projetadas para invalidar termos inaceitáveis). Dentre as regras procedimentais estão a renúncia explícita e escrita, a utilização de linguagem simples e a indicação do valor monetário da renúncia, o aconselhamento especializado independente antes da decisão, a concessão de prazo para reflexão, a possibilidade de o empregado revogar o consentimento a qualquer tempo ou a expiração do consentimento depois de um certo período, a negociação coletiva e a aprovação pelo poder público, sendo essas duas últimas proteções consideradas mais fortes do que as demais, por contarem com uma validação externa. E entre as regras substantivas são citados os testes de proporcionalidade e o padrão de racionalidade[148].

Para Davidov a combinação entre as regras procedimentais ("procedural rules") e as regras substantivas ("substantive rules") é a melhor forma de encarar o problema, pois aumenta-se a probabilidade de o consentimento ser livre e informado e de serem invalidados acordos inaceitáveis.

Deve-se partir da presunção de que qualquer renúncia a direito trabalhista é imposta ao trabalhador, incumbindo ao empregador provar o contrário. Assim, não observadas as justificações procedimentais e/ou substantivas, é aconselhável que o consentimento dado pelo empregado seja invalidado.

---

147 Guy Davidov – Non-waivability in Labour Law. *Oxford Journal of Legal Studies*. Vol. 40, nº 3 (2020), p. 10-18.

148 Guy Davidov – 7º Encontro Ibérico Transformações Recentes. Disponível em: https://www.youtube.com/watch?v=0Y8b0o7TLPA&t=8288s (9.5.2022).

Segundo Maria Raquel Guimarães e Maria Regina Redinha, a renúncia será admissível se não houver ofensa à dignidade humana e quando for resultado da expressão de consentimento livre e informado[149]. Isso significa dizer que o desequilíbrio de poder inerente à relação laboral não inibe a liberdade de escolha do empregado perante toda e qualquer circunstância, mas o empregador precisa adotar as salvaguardas adequadas.

Nos tópicos que se seguem abordaremos mais detidamente o consentimento do trabalhador como base legal de tratamento dos seus dados pessoais.

10.1. DELIMITAÇÃO TEMÁTICA DO CONSENTIMENTO

Embora o consentimento já estivesse previsto em algumas legislações nacionais como um dos fundamentos legais para o tratamento de dados pessoais desde os anos setenta, esta abordagem não encontrou expressão na Convenção n. 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, considerado o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados.[150]

No âmbito da União Europeia, entretanto, desde o início do processo legislativo que culminou com a Directiva 95/46/CE, o consentimento apareceu como fundamento legal para o tratamento de dados. Ele também está amparado no art. 8, n. 2, da Carta dos Direitos Fundamentais da União Europeia, que estabelece, desde logo, que esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei, bem como no n. 3 do art. 35 da CRP.

O RGPD também atribuiu relevância jurídica ao consentimento, ao inseri-lo dentre as condições de licitude para o tratamento dos dados pessoais, a teor dos artigos 6 e 9, e defini-lo, no n. 11 do art. 4.º, como sendo "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento", elementos esses que serão aprofundados nos termos abaixo.

a) Manifestação de vontade livre

Como salientado, a manifestação de vontade terá de ser livre. E, de acordo com o considerando 42, RGPD, ela não o será se o titular dos dados não dis-

[149] Maria Raquel Guimarães; Maria Regina Redinha – A Portuguese approach to privacy in Covid-19 times: through the keyhole. In Ewoud HONDIUS [et al.]. *Coronavirus and the law in Europe*. Intersentia, 2021. p. 1022.

[150] Grupo de Trabalho de Proteção de Dados do Art. 29. Parecer nº 15/2011, sobre a definição de consentimento, adotado em 13 julho de 2011, WP187, p. 5. Disponível em: https://www.gpdp.gov.mo/uploadfile/others/wp187_pt.pdf (19.7.2022).

puser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado.

A referência que se faz à ausência de "uma escolha verdadeira ou livre" nos remete, de forma automática, para o universo da coação. Entretanto, a ausência de liberdade não se circunscreve a situações em que a vontade tenha sido exteriorizada debaixo de ameaças[151]. De um modo geral, qualquer circunstância que constitua pressão ou influência inadequada sobre o titular dos dados e que o impeça de exercer livremente a sua vontade tornará o consentimento inválido, e isso se pode manifestar das mais diversas maneiras[152].

É assim que no contexto laboral, marcado por um desequilíbrio de poder entre empregadores e empregados, ressalvadas raras exceções, é bastante improvável que o consentimento seja manifestado de forma inteiramente livre[153], nos termos supra expostos a propósito dos limites da indisponibilidade no contexto laboral.

Neste sentido, aliás, é o considerando 43, RGPD, para o qual o consentimento não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento.

Aprofundando-se na avaliação da liberdade do consentimento, o n. 4 do art. 7, RGPD, determina que há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um ser-

---

151 Barreto Menezes António Cordeiro – *O consentimento do titular dos dados no RGPD*. Lisboa: Universidade de Lisboa, 2018. Disponível em: https://blook.pt/publications/publication/e772e2d8f7b4/ (19.7.2022).

152 Grupo de Trabalho do Art. 29 para a Proteção de Dados. Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, WP 259 rev.01), adotada em 28 nov. 2017, por último revisto a 10 abr. 2018, p. 6. Disponível em: https://www.uc.pt/protecao-de-dados/suporte/20180411_orientacoes_relativas_a_transparencia_wp260_rev01#:~:text=Este%20grupo%20de%20trabalho%20foi,Diretiva%202002%2F58%2FCE (19.7.2022).

153 Sobre o ponto, pertinentes as orientações propostas pelo Grupo de Trabalho do Art. 29: "Atendendo à dependência que resulta da relação empregador/trabalhador, é improvável que o titular dos dados possa recusar ao seu empregador o consentimento para o tratamento dos dados sem que haja medo ou risco real de consequências negativas decorrentes da recusa. É improvável que um trabalhador responda livremente ao pedido de consentimento do empregador para, por exemplo, ativar sistemas de controlo como a observação do local de trabalho através de câmaras ou preencher formulários de avaliação, sem sentir qualquer tipo de pressão para dar esse consentimento. Por conseguinte, o GT29 considera problemática a questão de os empregadores procederem ao tratamento de dados pessoais dos seus trabalhadores atuais ou futuros com base no consentimento, uma vez que é improvável que esse consentimento seja dado de livre vontade. Relativamente à maior parte deste tratamento de dados no local de trabalho, o fundamento legal não pode nem deve ser o consentimento dos trabalhadores [artigo 6.º, n.º 1, alínea a)], devido à natureza da relação entre empregador e trabalhador". Grupo de Trabalho do Art. 29 para a Proteção de Dados. Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679. p. 7.

viço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato.

Nos termos deste dispositivo, pretende-se assegurar que a finalidade do tratamento dos dados pessoais não está camuflada nem agregada à execução de um contrato ou à prestação de um serviço para os quais esses dados pessoais não são necessários. Ou seja, tem de existir uma relação direta e objetiva entre o tratamento dos dados e a finalidade da execução do contrato.[154]

Diante dessa lógica, estipula o Código do Trabalho, nos seus artigos 17 e 18, que informações sensíveis respeitantes à vida privada do trabalhador ou candidato a emprego só podem ser recolhidas quando estritamente necessárias e relevantes para a execução do contrato de trabalho. Sobre o assunto, Maria Regina Redinha esclarece que há de ser obedecido um critério de proporcionalidade e adequação para a obtenção de informações, devendo ser recolhidas apenas aquelas informações que tenham imediata relevância para as finalidades que o legislador considera objectivamente justificáveis da derrogação do princípio de reserva de intimidade da vida privada[155].

Segundo o mesmo considerando 43, RGPD, anteriormente citado, há uma presunção de que o consentimento não é livre se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.

Além de prever a questão da condicionalidade mencionada pelo n. 4 do art. 7, RGPD, o considerando 43, RGPD, dispõe acerca da granularidade, que, em outros termos, significa dizer que o titular de dados deve poder escolher para quais finalidades específicas está dando o seu consentimento. Prosseguindo nessa mesma ideia, determina o considerando 32, RGPD, que o consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade, sendo que nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins.

Outro indicativo na identificação de se o consentimento é realmente livre é analisar se a recusa ou retirada do consentimento provocará ou não prejuízos (materiais e/ou morais[156]) ao titular de dados. Se o responsável pelo tratamento for capaz de demonstrar que o serviço inclui a possibilidade de retirar o consentimento sem que daí advenham quaisquer consequências negativas, nomeadamente que a prestação do serviço perca qualidade pre-

154 *Ibid.*, p. 8-9.

155 Maria Regina Gomes Redinha. Da Protecção da Personalidade no Código do Trabalho. *Para Jorge Leite*: escritos jurídico-laborais. Coimbra: Coimbra Editora, 2014. p. 880-881.

156 Diogo Filipe Rodrigues Da SILVA – *Regulamento Geral de Proteção de Dados*: O Consentimento do Trabalhador. Porto: Out. 2020. Dissertação conducente à obtenção do Grau de Mestre em Direito pela Faculdade de Direito da Universidade do Porto.

judicando o utilizador, tal pode servir para comprovar que o consentimento foi dado livremente[157].

De maneira sintética, o GT 29 defende que sempre que a ausência do consentimento puder acarretar relevantes prejuízos reais ou potenciais ao trabalhador, de modo que este não tenha a possibilidade efetiva de recusá-lo, então o consentimento não será livre e, consequentemente, válido[158].

b) Manifestação de vontade dirigida

Por força do art. 6, n. 1, al. *a)*, RGPD, para que o tratamento de dados seja lícito, é preciso que o titular dos dados direcione o seu consentimento para uma ou mais finalidades específicas.

Cumpre notar que a vontade em si é um processo volitivo interno da pessoa, somente adquirindo relevância jurídica através da sua exteriorização, quando o indivíduo dirige ou preordena a sua vontade para uma finalidade específica.

O consentimento dirigido – ou específico, segundo a terminologia do RGPD - está intrinsecamente relacionada com a noção de limitação da finalidade que consta do artigo 5, n. 1, al. *b)*, RGPD, segundo a qual os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas e não podem ser tratados posteriormente de uma forma incompatível com essas finalidades.

Para o GT 29, o cumprimento deste elemento compreende três dimensões: *(i)* especificação em função da finalidade como salvaguarda contra o desvirtuamento da função, *(ii)* granularidade nos pedidos de consentimento, e *(iii)* separação clara entre as informações relacionadas com a obtenção de consentimento para atividades de tratamento de dados e as informações sobre outras questões[159].

Esse requisito constitui, portanto, importante mecanismo de controlo do titular dos dados sobre o processamento deles, não sendo permitido ao responsável pelo tratamento utilizá-los para finalidade diversa daquela para a qual o titular preordenou a sua vontade.

c) Manifestação de vontade informada

Para que o tratamento de dados seja legítimo, é necessário, ainda, que o consentimento seja informado. Ou seja, antes da obtenção do consentimento por parte do titular dos dados, é necessário que sejam suficientemente

---

157 Grupo de Trabalho do Art. 29 para a Proteção de Dados. Orientações relativas ao consentimento na aceção do Regulamento. p. 12.

158 Grupo de Trabalho do Art. 29, Parecer nº 15/2011, sobre a definição de consentimento, adotado em 13 julho de 2011, WP187, p. 15. Disponível em: https://www.gpdp.gov.mo/uploadfile/others/wp187_pt.pdf (19.7.2022).

159 Grupo de Trabalho do Art. 29. Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, p. 13.

esclarecidos para que possam tomar decisões efetivamente informadas. A pessoa em causa precisa compreender verdadeiramente para o que está dando o seu consentimento e as implicações que ele pode ocasionar.

Nesse ponto, assume especial relevância os princípios da licitude, lealdade e transparência, consagrados no n. 1, al. *a)* do art. 5 do RGPD.

Com esteio no art. 13 do RGPD, o GT 29 considera como necessárias para se obter um consentimento válido as seguintes informações: "*(i)* identidade do responsável pelo tratamento, *(ii)* a finalidade de cada uma das operações de tratamento em relação às quais se procura obter o consentimento31, *(iii)* que (tipo de) dados serão recolhidos e utilizados, *(iv)* existência do direito de retirar o consentimento, *(v)* informações acerca da utilização dos dados para decisões automatizadas em conformidade com o artigo 22.º, n.º 2, alínea c), quando pertinente, e *(vi)* sobre os possíveis riscos de transferências de dados devido à inexistência de uma decisão de adequação e de garantias adequadas, tal como previsto no artigo 46.º"[160]

Para que o consentimento seja, de fato, informado, é preciso que as informações sejam fornecidas ao titular dos dados de modo inteligível e de fácil acesso e numa linguagem clara e simples (art. 7, n. 2, e considerando 32, ambos do RGPD), devendo o titular dos dados ser informado de que tem o direito de retirar o seu consentimento a qualquer momento (art. 7, n. 3, RGPD).

d) Manifestação de vontade inequívoca

Por fim, consoante os termos do art. 4, n. 11, RGPD, para que o consentimento seja válido é exigida uma manifestação de vontade explícita, mediante declaração ou ato positivo inequívoco. Ou seja, não pode haver dúvida de que o titular dos dados deu o seu consentimento para o tratamento em causa.

O considerando 32, RGPD, traz contornos esclarecedores sobre o ponto, ao estabelecer que o consentimento do titular dos dados deverá ser dado mediante um ato positivo claro, que pode se traduzir tanto numa declaração escrita, inclusive em formato eletrónico, como numa declaração oral (gravada). O silêncio, as opções pré-validadas ou a omissão não serão considerados manifestações inequívocas e, portanto, o consentimento obtido sob tais formas não será válido.

Segundo as orientações do GT 29, a aceitação generalizada de condições gerais do contrato ou a apresentação de opções pré-assinaladas que exijam a intervenção do titular dos dados para impedir a aceitação não pode ser encarado como ato positivo inequívoco[161].

---

[160] Grupo de Trabalho do Art. 29 para a Proteção de Dados. Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679. p. 14-15.

[161] Grupo de Trabalho do Art. 29 para a Proteção de Dados. Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679. p. 18.

Em relação ao tratamento de dados sensíveis, além de todos esses requisitos, o consentimento deve, ainda, ser explícito, ou seja, exigirá uma expressão de vontade precisa, seja escrita ou oral[162], porquanto há uma maior exigência do consentimento prestado nos termos do n. 2 do art. 9, em comparação à noção de consentimento vertida no ponto 11 do artigo 4 e que é pressuposta pela alínea *a)* do n. 1 do art. 6, todos do RGPD.

10.2. O CONSENTIMENTO COMO BASE LEGAL PARA O TRATAMENTO DOS DADOS DOS TRABALHADORES

Como oportunamente já chamamos atenção, muitas das atividades rotineiramente realizadas no contexto laboral envolvem o tratamento de dados pessoais dos trabalhadores. Mesmo antes da formação da relação de trabalho, quando do processo de recrutamento, os dados pessoais dos candidatos a emprego são recolhidos pelo potencial empregador; esse tratamento continua durante todo o contrato de trabalho para as mais diversas finalidades, dentre as quais podemos citar a elaboração da folha de pagamento, os registos relativos a doenças e acidentes de trabalho ou relacionados à promoção, transferência e treinamento e tantos outros imprescindíveis para o desempenho da relação de trabalho ou para cumprimento das obrigações legais a que o empregador está sujeito; e, embora a recolha dos dados pessoais do trabalhador finde com o término do contrato de trabalho, é possível que se procedam a outras operações envolvendo esses dados, como, por exemplo, para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

O GT 29, no Parecer 8/2001, sobre o tratamento de dados pessoais no contexto laboral, salienta que a interação entre a lei de proteção de dados e a relação trabalhista aumenta gradativamente com o desenvolvimento do uso da tecnologia da informação e comunicação no emprego. Seja através da utilização de e-mail, acesso à internet, câmeras de vídeo ou dados de localização, não resta dúvida de que o processamento de dados pessoais é uma realidade bastante presente na prática trabalhista, cabendo ao aplica-

---

[162] Para a versão inglesa do RGPD, o conceito de consentimento previsto na alínea a) do nº 2 do art. 9º é qualificado em relação à noção prevista no art. 4º, ponto 11) pela necessidade de, para além de inequívoco, ser explícito e para finalidades específicas. Já para a tradução portuguesa do RGPD, sendo o consentimento *explícito* em ambos os casos, a distinção entre o consentimento para o tratamento de categorias de dados sensíveis e não sensíveis requer um esforço de criatividade do intérprete – ou, em alternativa, a consulta da versão inglesa do RGPD. Alexandre Sousa Pinheiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina, 2018. p. 247-248. A inclusão da expressão "explícita" na versão portuguesa do art. 4º, 11, deve ser desconsiderada, pois trata-se de um manifesto erro de escrita, como esclarece: António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 136.

dor do direito encontrar soluções jurídicas que protejam adequadamente os interesses desses trabalhadores.

Pois bem. Para que o tratamento de dados seja lícito, é preciso o enquadramento numa das bases legais autorizativas do art. 6, RGPD, em se tratando de dados pessoais não sensíveis - ou, em se tratando de dados sensíveis, a recondução a uma das exceções elencadas no n. 2 do art. 9 do RGPD -, sendo o consentimento dado pelo titular dos dados fundamento legal para o tratamento de ambas as categorias.

No entanto, como retro exposto, é necessário que esse consentimento seja válido, ou seja, ele deve ser livre de qualquer coação da vontade, específico em relação à finalidade do tratamento, informado em relação ao tratamento dos dados que tenham sido facultados e inequívoco, no sentido de não deixar qualquer margem para dúvidas em relação ao sentido da vontade do declarante.

Ocorre que diante da subordinação jurídica que permeia a relação laboral - que se traduz objetivamente na sujeição do trabalhador à autoridade e direção do empregador - e do consequente temor do empregado ou do candidato a emprego de sofrer retaliações por parte do empregador, o tratamento de dados pessoais baseado no consentimento é objeto de grande debate no contexto laboral[163]. Existe uma certa presunção de que o consentimento dado nesse contexto é frágil, pois raramente será livre, já que o titular dos dados/trabalhador dificilmente disporá de uma escolha verdadeira ou livre e poderá recusar retirar o consentimento sem ser prejudicado, à luz do que preceitua o considerando 42, RGPD.

O próprio RGPD mostrou preocupação quanto a tal questão, ao prever, em seu considerando 43, que o consentimento não constitui fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento.

Dessa maneira, tem-se entendido que o consentimento no contexto laboral deve ser utilizado apenas em última instância, quando nenhum dos outros fundamentos legais puderem ser invocados, e, sobretudo, quando não houver qualquer risco de o empregado sofrer retaliações ou consequências negativas pela recusa do seu consentimento. Para ilustrar uma situação em

163 "No domínio do tratamento de dados sensíveis em contexto laboral, podemos verificar a tensão entre duas dimensões da subordinação jurídica. Por um lado, o desequilíbrio de posições entre empregador e trabalhador gera a necessidade de criar garantias especialmente exigentes, atenta a vulnerabilidade do segundo em relação a decisões do primeiro a respeito do tratamento dos seus dados pessoais. Por outro lado, o tratamento de dados considerados sensíveis pode apresentar-se como um meio de garantir direitos e interesses dos trabalhadores, concretizados em obrigações jurídicas do empregador, nomeadamente no que concerne às normas de segurança, higiene e saúde no trabalho". Alexandre Sousa Pinheiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina, 2018. p. 281-282.

que o consentimento pode ser tido como verdadeiramente livre, cito exemplo elaborado pelo Grupo de Trabalho do Artigo 29:

> Uma equipa de filmagem pretende filmar determinada parte de um escritório. O empregador solicita o consentimento de todos os trabalhadores que se sentam nessa zona do escritório para serem filmados, uma vez que podem aparecer em segundo plano nas filmagens do vídeo. Os trabalhadores que não quiserem ser filmados não serão de forma alguma penalizados, uma vez que serão colocados noutro local de trabalho equivalente numa outra zona do edifício enquanto durar a filmagem.[164]

Portanto, diante da típica assimetria existente nas relações laborais, nas quais o titular de dados é o trabalhador, geralmente, a parte mais fraca da relação jurídica estabelecida, considera-se que o consentimento dado nesse contexto não será, na grande maioria dos casos, o fundamento mais apropriado para o tratamento dos dados pessoais dos trabalhadores.

Segundo Diogo Pereira Duarte as reservas em torno do consentimento no contexto laboral implicaram, em geral, a ênfase do tratamento fundado no interesse legítimo do responsável pelo tratamento, na medida em que os demais fundamentos apenas permitem cobrir um conjunto básico de operações de tratamento por parte do empregador[165]. Seja como for, tais reservas não impedem que os dados pessoais dos trabalhadores sejam objeto de tratamento, porquanto o consentimento não possui qualquer papel prioritário, é, antes, "apenas mais uma das estruturas base da licitude do tratamento e não uma exigência absoluta para se lograr processar dados pessoais"[166].

Assim, com vistas a evitar acusações de invalidade do consentimento dado pelo empregado e ressalvada a hipótese de inexistência de qualquer risco de o empregado sofrer retaliações ou consequências negativas pela recusa do seu consentimento, é preferível que o responsável pelo tratamento, o empregador, apenas invoque o consentimento quando não exista outro fundamento que o justifique. Dito de outro modo, apenas quando existam garantias de que o consentimento é verdadeiramente livre é que ele poderá ser invocado como fundamento legítimo para o tratamento de dados pessoais dos trabalhadores.

Por conseguinte, é preciso uma análise atenta e cuidadosa do contexto para que se possa identificar que o consentimento se afigura como base adequada para o processamento dos dados dos trabalhadores. Se utilizado corretamente, ele funciona como importante instrumento de controlo da

---

164 Grupo de Trabalho do Art. 29 para a Proteção de Dados. Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679. p. 8.

165 Diogo Pereira Duarte – In António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 526.

166 Diogo Filipe Rodrigues Da SILVA – *Regulamento Geral de Proteção de Dados*: O Consentimento do Trabalhador. Porto: Out. 2020. Dissertação conducente à obtenção do Grau de Mestre em Direito pela Faculdade de Direito da Universidade do Porto.

pessoa em causa sobre o tratamento dos seus dados; em contrapartida, se utilizado incorretamente, esse controlo torna-se ilusório[167] e pode ensejar, no final das contas, uma vulnerabilidade ainda maior da posição da pessoa-trabalhadora. A relevância do consentimento como um factor da autonomia e autodeterminação do titular dos dados baseia-se, portanto, no seu uso no contexto certo, devendo estar reunidos os elementos necessários para se chegar a tal conclusão[168].

a) A deliberação 2019/494 da CNPD

A Comissão Nacional de Proteção de Dados (CNPD) é a autoridade de controlo nacional em matéria de proteção de dados (art. 3 da Lei 58/2019). Ela consiste numa entidade administrativa independente, em funcionamento junto da Assembleia da República, que controla e fiscaliza o cumprimento do RGPD, da Lei 58/2019, da Lei 59/2019 e da Lei 41/2004, bem como das demais disposições legais e regulamentares relativas à proteção de dados pessoais, a fim de defender os direitos e liberdades das pessoas singulares no que diz respeito ao tratamentos dos seus dados pessoais (art. 51 do RGPD c/c art. 4 da LE)[169].

Por meio da Deliberação 2019/494, de 03 de setembro de 2019, a qual define o entendimento desta entidade reguladora perante algumas das normas da Lei n. 58/2019 (lei que assegura a execução, na ordem jurídica nacional, do RGPD), a CNPD decidiu por desaplicar, nas situações de tratamento de dados pessoais que venha a apreciar, a alínea *a)* do n. 3 do artigo 28 da referida legislação - que estabelece que, salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador.

A CNPD entendeu que este dispositivo traduz uma limitação excessivamente restritiva do consentimento do trabalhador, na medida em que elimina qualquer margem de livre arbítrio dos trabalhadores, mesmo quando há condições para a sua manifestação sem risco para os seus direitos e interesses, na contramão, aliás, do posicionamento perfilhado pelo GT 29, que defende que os trabalhadores podem dar o seu consentimento livremente em circunstâncias excecionais, quando o ato de dar ou recusar o consentimento não produzir quaisquer consequências negativas.

Indo mais além, a CNPD concluiu que, por traduzir uma restrição não adequada, desnecessária e excessiva do direito fundamental à autodetermina-

---

[167] Parecer nº 15/2011, sobre a definição de consentimento, adotado em 13 julho de 2011, WP187, p. 2. Disponível em: https://www.gpdp.gov.mo/uploadfile/others/wp187_pt.pdf (19.7.2022).

[168] *Ibid.*, p. 37.

[169] Disponível em: https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/ (10.5.2022).

ção informacional ou à proteção dos dados enquanto direito ao controlo dos seus próprios dados, para lá do que é necessário à salvaguarda dos direitos e interesses dos trabalhadores, a norma restringiu o âmbito de aplicação da alínea *a)* do n. 1 do artigo 6 e da alínea *a)* do n. 2 do artigo 9 do RGPD, e violou, por via de consequência, o princípio do primado do Direito da União Europeia.

De outro lado, chama-se atenção para o fato de que, antes da entrada em vigor do RGPD, vigorava o princípio da hetero-regulação, competindo à CNPD, enquanto autoridade de controlo, registar ou autorizar o tratamento de dados pessoais em determinadas situações específicas. É o que estabelece o art. 18, n. 1, CT, quando condiciona o tratamento de dados biométricos do trabalhador pelo empregador após notificação à Comissão Nacional de Protecção de Dados. Porém, com a entrada em vigor do RGPD desapareceu essa obrigação de notificação prévia à CNPD para o tratamento de dados biométricos, não restando mais à autoridade de controlo nacional qualquer função reguladora, mas apenas fiscalizadora e orientadora, nos termos preconizados pelos artigos 57 do RGPD, 6 da Lei 58/2019 e 44 da Lei 59/2019.[170]

Assim, ao mesmo tempo em que o disposto no art. 28, n. 3, al. *a)*, da Lei n. 58/2019 restringiu de maneira desproporcional o recurso ao consentimento inclusive para as situações em que não há qualquer risco para os direitos e interesses dos trabalhadores, tem-se, também, que a CNPD excedeu o limite de suas atribuições e competências, na medida em que hoje lhe é atribuível um papel meramente fiscalizador em matéria de proteção de dados.

11. OS DADOS RELACIONADOS À SAÚDE DO EMPREGADO

Dentre os dados sensíveis que nos interessam em específico no presente trabalho estão os dados relativos à saúde, que, segundo o ponto 15 do art. 4 do RGPD, são os "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde".

A Constituição da Organização Mundial de Saúde (OMS) possui uma definição ampla do termo 'saúde', afirmando que esta não consiste apenas na ausência de doença ou de enfermidade, mas compreende um estado de completo bem-estar físico, mental e social[171].

---

[170] Diogo Filipe Rodrigues Da SILVA – *Regulamento Geral de Proteção de Dados*: O Consentimento do Trabalhador. Porto: Out. 2020. Dissertação conducente à obtenção do Grau de Mestre em Direito pela Faculdade de Direito da Universidade do Porto. Ver também: https://www.sociedadeadvogados.eu/pt/comunicacao/a-recolha-de-dados-biometricos-no-contexto-laboral/704/.

[171] § 2º do preâmbulo da Constituição da OMS.

O direito à proteção da saúde está consagrado no art. 64 da CRP como direito fundamental social, estando inserido no catálogo dos direitos económicos, sociais e culturais. A CRP atribui uma grande importância jurídica ao bem jurídico 'saúde', pois além de possuir óbvia relação com outros direitos fundamentais, como o direito à vida (art. 24) e o direito à integridade pessoal (art. 25)[172], existem outras normas constitucionais que (lateralmente) também protegem o bem jurídico 'saúde'[173], como é o caso do direito à prestação do trabalho em condições de higiene, segurança e saúde, do direito dos consumidores à proteção da saúde e do direito a um ambiente sadio.

O Tribunal de Justiça da União Europeia (TJUE) tem compreendido que a expressão "dados relativos à saúde" deve ser interpretada em sentido lato[174]. Tal como indicado no considerando 53, RGPD, os dados relativos à saúde, por pertencerem às categorias especiais de dados pessoais, merecem uma proteção mais elevada, haja vista que o tratamento desses dados pode ter impactos negativos significativos para os titulares dos dados. Referem-se, segundo o considerando 35, RGPD, a todas as informações sobre a saúde física ou mental do titular dos dados no passado, no presente ou no futuro[175]. Além disso, não importa se esses dados revelem uma informação positiva ou negativa, bastando que diga respeito à saúde do respectivo do titular, e não que evidencie propriamente uma eventual doença[176].

Apesar de os dados de saúde não constarem no elenco do art. 35 da CRP[177], o Acórdão do Tribunal Constitucional n. 355/97 compreendeu que os dados de saúde são dados sensíveis por integrarem a categoria de dados relativos à vida privada, tais como as informações referentes à origem étnica, à vida familiar, à vida sexual, condenações em processo criminal, situação patrimonial e financeira, sendo, aliás, posteriormente consagrados como tal de forma expressa pelo art. 7 da Lei nº 67/98 (Lei da Protecção de Dados Pessoais), que transpôs para a ordem jurídica portuguesa a Directiva

---

172 Rui Medeiros – Anotação ao artigo 64º. In Jorge Miranda; Rui Medeiros – *Constituição Portuguesa Anotada*. Vol. I, 2ª ed. revista. Coimbra: Coimbra Editora, 2010. p. 1308-1310.

173 Maria João Estorninho; Tiago Macieirinha – *Direito da saúde*. Lisboa: Universidade Católica, 2014. p. 33.

174 Diretrizes nº 03/2020 sobre o tratamento de dados relativos à saúde para efeitos de investigação científica no contexto do surto de COVID-19. Adotadas em 21 de abril de 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_pt.pdf (19.7.2022).

175 Considerando 35 do RGPD.

176 António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 95.

177 A Constituição estipula, para fins de proteção de dados pessoais, uma graduação dos bens jurídicos consoante um critério de reserva privada. Ao alencar expressamente as convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica (art. 35º, nº 3), tem-se que estes bens são objeto de uma tutela constitucional acrescida. Alexandre Sousa Pinheiro – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 756.

n. 94/46/CE. E não poderia deixar de ser assim, pois, como bem adverte Alexandre Sousa Pinheiro, "os dados de saúde como expressão directa do princípio da dignidade da pessoa humana, têm uma tutela constitucional idêntica aos restantes dados pessoais enunciados no art. 35º, nº 3."[178].

Interessante notar que os dados relativos à saúde correspondem à categoria prevalente de dados tratados com a finalidade de avaliar a capacidade para o trabalho, mormente porque, a teor do disposto no n. 1 do art. 108 da Lei n. 102//2009, a avaliação da aptidão é efetuada através da realização de exames de saúde[179]. Sobre o ponto, o Tribunal Constitucional considerou que não era inconstitucional a previsão legal de exames médicos destinados à verificação da aptidão física e psíquica do trabalhador para o exercício da sua profissão, bem como as fichas "clínicas" e de "aptidão"[180]. Mas considerou que o acesso directo por parte do empregador às informações relativas à saúde ou estado de gravidez violavam o direito fundamental de reserva à intimidade da vida privada[181].

O tratamento de dados relativos à saúde, enquanto dados especiais, é regulado pelo artigo 9 do RGPD, dispositivo este que proíbe o tratamento desta categoria de dados, salvo se o tratamento puder ser reconduzido a uma das exceções previstas no n. 2 do respectivo enunciado normativo.

Como dito, o n. 2 do art. 9, RGPD, prevê derrogações ao princípio geral da proibição do tratamento de dados sensíveis, dentre as quais podemos destacar o consentimento explícito do titular de dados e as hipóteses em que o tratamento é necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, bem como para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado. As derrogações previstas não são cumulativas e, portanto, não é exigido o consentimento explícito do titular quando houver outra base autorizativa para o tratamento, mesmo porque, como já analisamos no tópico anterior, o consentimento do trabalhador para o tratamento de dados pessoais, especialmente quando se está perante dados sensíveis, é questão bastante delicada no contexto laboral e que suscita dúvidas porquanto raramente a manifestação de vontade do empregado será livre.

Convém mencionar que o empregador não pode exigir ao candidato a emprego ou ao trabalhador que preste informações relativas à sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à natureza da actividade profissional o justifiquem e seja fornecida por escrito a respectiva fundamentação (alínea *b)* do n. 1 do art. 17, CT.

---

178 Alexandre Sousa PINHEIRO – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015. p. 760.

179 Alexandre Sousa PINHEIRO (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina, 2018. p. 316.

180 Acórdão nº 368/02 do Tribunal Constitucional.

181 Acórdão nº 306/03 do Tribunal Constitucional.

Em que pese o titular tenha o direito de que certos fatos da sua vida não sejam revelados, o médico do trabalho pode ter acesso a aspectos relativos à vida privada do trabalhador, relacionados ao seu estado de saúde, mormente porque a reserva da vida privada não é um direito absoluto e desse modo precisa ser compatibilizado com outros interesses constitucionalmente consagrados, à luz do que preconiza o art. 18, n. 2, CRP. Neste contexto, a restrição ao direito à privacidade do trabalhador é justificada sempre que seja necessária para verificar a aptidão física e psíquica para o desenvolvimento da atividade e para fins de proteção e segurança do trabalhador ou de terceiros.

Assim sendo, a determinação da finalidade e o consequente tratamento desses dados não está na disponibilidade do empregador, na medida em que a licitude do tratamento dos dados relativos à saúde depende do enquadramento numa das exceções legais, além de estar sujeito às devidas salvaguardas[182]. Com efeito, do mesmo modo que não podemos conceber uma reserva absoluta do titular/trabalhador se sobrepondo à obrigação que recai sobre o empregador de desenvolver a sua atividade em condições de segurança, higiene e saúde no trabalho, também não podemos aceitar o acesso irrestrito e ilimitado por parte do empregador aos dados de saúde de seus empregados.

O ponto 9.2 da Recomendação CM/Rec(2015)5 do Comité de Ministros aos Estados membros sobre o tratamento de dados pessoais no contexto do emprego, alerta que o empregador apenas poderá licitamente pretender aceder a informação relativa ao estado de saúde do candidato ou do trabalhador, ou solicitar a qualquer um deles a realização de exames, por ou sob a responsabilidade do médico do trabalho, para: *a)* verificar sua aptidão para determinado posto de trabalho, presente ou futuro; *b)* cumprir as normas da medicina preventiva; *c)* garantir a reabilitação adequada, ou cumprir qualquer outra disposição relativa ao ambiente de trabalho; *d*) salvaguardar os interesses vitais do titular dos dados, de outros trabalhadores, ou de terceiros; *e)* possibilitar a concessão de benefícios sociais; *f)* contestar processos judiciais[183].

O sigilo a que está sujeito o médico do trabalho[184] que tem acesso às informações relativas ao estado clínico do trabalhador funciona como importante garantia ao titular dos dados, na medida em que a sua inobservância pode

---

182 Conforme ponto 9.4 da Recomendação CM/Rec(2015)5 do Comité de Ministros aos Estados membros sobre o tratamento de dados pessoais no contexto do emprego. Adotada em 1º de abril de 2015. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a (15.2.2022).

183 Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a (15.2.2022).

184 "A entidade não deve ter acesso ao boletim médico, mas apenas às recomendações do médico do trabalho resultantes do exame médico, que devem ser vertidas na ficha de aptidão, a entregar ao responsável dos recursos humanos da empresa". Prossegue afirmando que "para além de vigiar a saúde dos trabalhadores, o médico do trabalho é o garante da confidencialidade das informações e da salvaguarda dos princípios do tratamento dos dados sensíveis e, consequentemente, da proteção da vida privada e da proibição da

ensejar práticas discriminatórias tanto em face dos trabalhadores como em face dos candidatos a emprego (*v.g.*, quando o médico do trabalho informa ao empregador que o empregado é portador do vírus HIV e em decorrência disso ele é dispensado)[185]. Esse quadro torna-se ainda mais problemático quando o médico do trabalho é contratado pela própria empresa ou integra a sua estrutura, cabendo-lhe, neste caso, ponderar entre os seus deveres perante o paciente/trabalhador e as suas obrigações diante da empresa.

Outra questão que merece reflexão diz respeito aos desdobramentos de procedimentos médicos aparentemente inócuos, que, diante do avanço da tecnologia, permitem o conhecimento de uma infinidade de informações sobre o indivíduo, desde a análise do seu estado de saúde atual até a averiguação de possíveis doenças que possam vir a se desenvolver no futuro[186]. O conhecimento de um risco médico, por meio de um teste genético[187] (*v.g.*, se determinada pessoa apresenta propensão ou tendência elevada para uma série de condições hereditárias, de *Alzheimer* à Síndrome de *Zellweger*), pode ensejar práticas discriminatórias tanto em face da própria pessoa como de seus familiares[188].

Finalmente, um debate que se mostra bastante atual envolvendo o tratamento de dados de saúde do empregado gira em torno da testagem e da exigência de comprovante de imunização, no contexto da pandemia do COVID-19, tema que nos aprofundaremos nos tópicos seguintes.

---

discriminação". Alexandre Sousa Pinheiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina, 2018. p. 287.

185 No acórdão nº 368/02 do Tribunal Constitucional, destaca-se que "o médico do trabalho não pode transmitir ao empregador, sob pena de violação do segredo profissional, qualquer indicação que traduza um diagnóstico sobre o estado de saúde".

186 Rita Isabel Ramos Batista Escarpiado – *Discriminação do trabalhador em razão do conhecimento da informação médica*: em especial os dados genéticos. Lisboa: Universidade de Lisboa, 2018. Dissertação para a obtenção do grau de Mestre em Direito e Prática Jurídica, especialidade Direito da Empresa. Disponível em: https://repositorio.ul.pt/bitstream/10451/37504/1/ulfd137176_tese.pdf (30.11.2021).

187 Apesar de o histórico médico familiar estar compreendido no conceito de informações genéticas quando presente o risco de comunicação genética, importa salientar que informação genética e informação médica não se confundem. "Congress anticipated that plaintiffs might confuse biological conditions with genetic information and included a section in the statute expressly entitled 'Medical Information that Is Not Genetic Information'. This section explains that an employee's 'manifested disease, disorder, or pathological condition that has or may have a genetic basis' is *not* genetic information". Bradley A. Areheart, Jessica L – Gina Roberts, Big Data, and the Future of Employee Privacy. *The Yale Law Journal*. Vol. 128, nº 3 (2019), p. 710-791. Disponível em: https://www.yalelawjournal.org/pdf/AreheartRoberts_a2gvpzai.pdf (19.7.2022).

188 Bradley A. Areheart; Jessica L – Gina Roberts, Big Data, and the Future of Employee Privacy. *The Yale Law Journal.* Vol. 128, nº 3 (2019), p. 710-791. Disponível em: https://www.yalelawjournal.org/pdf/AreheartRoberts_a2gvpzai.pdf (19.7.2022).

12. A DISCUSSÃO EM TORNO DA RECUSA VACINAL E DA OBRIGATORIEDADE DA VACINAÇÃO

A atual situação pandêmica exigiu a adoção de medidas excepcionais para o enfrentamento e a mitigação do impacto econômico e social resultante da crise sanitária provocada pelo novo coronavírus.

Apesar de as vacinas COVID-19 carecerem de uma eficácia de 100% e não se saber por quanto tempo proporcionam imunidade, elas têm se mostrado a estratégia mais eficaz para prevenir a transmissão do vírus e salvar vidas[189]. A vacinação visa contornar um problema de saúde pública e a decisão de se vacinar ou não tem um impacto na sociedade como um todo e não apenas no indivíduo.

A vacinação, desde o seu surgimento até os dias atuais, reduziu drasticamente a incidência e a gravidade de doenças infecciosas. Em relação às doenças que se transmitem de pessoa para pessoa, a vacinação é benéfica tanto para o indivíduo - na medida em que lhe salvaguarda de doenças para a qual foi vacinado - como para a sociedade em geral – na medida em que atingido um determinado nível de vacinação na comunidade[190], tem-se o que se denomina por imunidade de grupo[191], ou seja, aquela situação em que, por virtude de imunidade, adquirida através de infecção e recuperação ou através da vacina, de uma determinada quantidade de pessoas na comunidade, já não é possível a transmissão do vírus de pessoa para pessoa, beneficiando-se diretamente desta imunidade de grupo também os indivíduos vulneráveis, que, por razões de saúde, não podem ser vacinados[192].

Como já mencionado, o direito à proteção da saúde é um direito social fundamental consagrado no art. 64 da CRP, e como tal encerra uma componente

---

189 De todo modo, ainda que a vacinação seja comprovadamente segura e eficaz, não é possível eliminar por completo os riscos de efeitos adversos provenientes dela, sendo importante, por isso mesmo, a instituição de um regime de responsabilização objetiva do Estado para o caso de indemnização de eventuais danos vacinais. João Carlos Carvalho Godinho – *A (re)discussão dos fundamentos da vacinação humana obrigatória*. Coimbra: Almedina, 2022. p. 55-56; Carla Amado Gomes – *Defesa da Saúde vs. Liberdade Individual*: casos da vida de um médico de saúde pública. Lisboa: Associação Académica da Faculdade de Direito de Lisboa, 1999. p. 88.

190 Para se atingir a imunidade de grupo, é preciso que uma percentagem muito grande da população esteja vacinada, variando consoante o agente infeccioso e as características da população, mas raramente é inferior a 85%, podendo mesmo atingir os 94% (no caso do sarampo e da tosse convulsa). João Carlos Carvalho Godinho – *A (re)discussão dos fundamentos da vacinação humana obrigatória*. Coimbra: Almedina, 2022. p. 63. *Apud* Paul E. Fine – Herd immunity: history, theory, practice. *Epidemiologic Reviews*. Vol. 15, nº 2 (1993), table 1, p. 268.

191 Para uma visão geral v. Artigo publicado no sítio eletrônico: https://dotlib.com/blog/o-que-e-imunidade-de-rebanho (3.2.2022).

192 Aquilino Paulo Antunes – Vacinas para a Covid-19: aspectos para reflexão. *Revista da Faculdade de Direito da Universidade de Lisboa*. Vol. 61, nº 2 (2020), p. 138.

subjetiva e uma componente objetiva. A subjetividade do direito fundamental está associada à faculdade de o indivíduo exigir a sua implementação aos poderes públicos, tanto através de ações como por omissões. Já a função objetiva reside no dever ou obrigação imposto ao Estado de assegurar o direito fundamental[193]. O próprio art. 64 não prevê apenas um direito à proteção da saúde, mas estabelece um dever de todos de a defender e promover.

O dever fundamental de defender e promover a saúde traz a relevância da saúde pública como valor comunitário constitucionalmente protegido, de modo que este dever tem como objeto a saúde pública, e não a saúde privada. De acordo com Carla Amado Gomes, "só na medida em que o mau estado de saúde de alguém possa reflectir-se no estado sanitário comunitário é que o Estado pode intervir, impondo determinados comportamentos (ou abstenção deles) ao cidadão doente"[194]. O Estado pode exigir que a pessoa contribua para a promoção da saúde comunitária, mas não pode obrigá-la a cuidar da própria saúde, sob pena de tolher o direito à autodeterminação do indivíduo e incorrer num paternalismo inaceitável[195].

Em que pese a saúde pública ser considerada um bem jurídico importante e a ciência demonstrar a todo tempo os inúmeros benefícios da vacinação, tanto individuais como coletivos, movimentos antivacinação[196], travestidos das mais diferentes motivações (religiosas, filosóficas ou até por mera desinformação) têm ganhado força, implicando um aumento no risco de propagação de doenças e até mesmo de mortes que poderiam ter sido evitadas com a vacina[197]. As pessoas que decidem não se vacinarem, por convicção

---

193 Sobre a dupla dimensão dos direitos fundamentais: João Carlos Vieira De ANDRADE – *Os Direitos fundamentais na Constituição Portuguesa de 1976*. 5ª ed. Coimbra: Almedina, 2016. p. 112.

194 Carla Amado Gomes – *Defesa da Saúde vs. Liberdade Individual*. Lisboa: Associação Acadêmica da Faculdade de Direito de Lisboa, 1999. p. 22-24.

195 João Carlos Carvalho Godinho – *A (re)discussão dos fundamentos da vacinação humana obrigatória*. Coimbra: Almedina, 2022. p. 55-56; Carla Amado Gomes – *Defesa da Saúde vs. Liberdade Individual*: casos da vida de um médico de saúde pública. Lisboa: Associação Acadêmica da Faculdade de Direito de Lisboa, 1999. p. 10-11.

196 Mesmo com os avanços obtidos e os resultados comprovados, o movimento anti-vacinação tomou força no fim da década de 70. As causas para o fortalecimento desse movimento ainda são motivo de intenso debate e de pesquisas, mas didaticamente pode-se dizer que os indivíduos antivacionistas se distribuem em espectros de dois polos: os ignorantes que não entendem o método científico e de conceitos matemáticos como risco e probabilidade e os que se utilizam do uso da desinformação e coação. Vitor Laerte Pinto Junior – Anti-vacinação, um movimento com várias faces e consequências. *Cadernos Ibero-Americanos de Direito Sanitário*. Brasília. Vol. 8, nº 2 (2019), p. 116-122.

197 "In December 2014, the first reported cases of measles arising in connection with Disneyland were reported. In the initial outbreak, fortytwo people visiting or working at Disneyland were exposed to measles.1 Measles is a highly communicable respiratory disease; the virus can linger on surfaces for up to two hours,2 which can be disastrous for an amusement park, school, or even a neighborhood playground. The virus mostly spread among

ou por dúvida quanto às características – de segurança ou eficácia – do produto[198], expõem a perigo não apenas a sua vida e a sua saúde, como também a vida e a saúde de outras pessoas.

Neste contexto, tendo em conta que a recusa vacinal pode colocar em causa a saúde pública, na medida em que pode prejudicar a imunidade de grupo e colocar em perigo outras pessoas, inclusive aquelas que são medicamente contraindicadas de se vacinar, tem-se discutido sobre a possibilidade de os órgãos competentes poderem intervir e tornar a vacinação obrigatória[199].

No panorama europeu, destaca-se o caso da Áustria, que foi o primeiro país da União Europeia a tornar obrigatória a vacina contra a COVID-19 para todos os adultos[200], a partir de fevereiro do corrente ano, estabelecendo pesadas sanções para aqueles que porventura recusem a vacinação, porém, após incisivas manifestações populares, a medida foi suspensa pouco mais de um mês após sua entrada em vigor[201].

Já o Parlamento francês substituiu o anterior passe sanitário (baseado tanto na vacinação como no teste negativo) pelo passaporte vacinal, este baseado exclusivamente na imunização com três ou duas doses da vacina com um atestado de restabelecimento após infecção com COVID-19 nos últimos seis meses, para entrar em locais públicos, sendo que, a partir de 14 de março, a medida também foi suspensa e agora apenas é exigida para instituições médicas, como hospitais, e lares de idosos[202].

Com efeito, a imposição da vacinação obrigatória, em prol da proteção do direito à saúde pública, precisa ser bem ponderada, pois a vacina constitui um procedimento em certa medida invasivo e que pode colidir com outros

---

those who had not been vaccinated, either because they were too young or were not vaccinated by choice." Erwin Chemerinsky; Michele Goodwin – *Compulsory Vaccination Laws Are Constitutional.* Legal Studies Research Paper Series Nº 2015-71. Vol. 110, nº 3 (2015), p. 590.

198 Aquilino Paulo Antunes – Vacinas para a Covid-19: aspectos para reflexão. *Revista da Faculdade de Direito da Universidade de Lisboa*. Vol. 61, nº 2 (2020), p. 146.

199 Examples of such disabilities could include a history of allergic reaction to vaccine ingredients, or an employees who are pregnant or nursing and have been advised against vaccination by a doctor. Margaret R. KURLINSKI – COVID-19: An Employer's Role in Vaccination. *Corporate Counsel*. Vol. 35, nº 1 (2021), p. 4-7.

200 Outras nações do bloco, como a Itália, por exemplo, obrigam a vacinação de uma parte da população ou de setores profissionais específicos. Disponível em: https://www.infomoney.com.br/minhas-financas/austria-e-1a-pais-da-europa-a-ter-vacinacao-obrigatoria-contra-covid-recusa-pode-gerar-multa-de-r-22-mil/ (19.7.2022).

201 Disponível em: https://cnnportugal.iol.pt/covid-19/vacinacao-obrigatoria-na-austria-com-efeitos-contrarios-autoridades-dizem-que-objetivo-nao-foi-cumprido/20720217/620e84330cf21a10a41fea7a. Ver também: https://www.dw.com/pt-br/%C3%A1ustria-suspende-obrigatoriedade-de-vacina-contra-covid-19/a-61068019 (19.7.2022).

202 Disponível em: https://www.publico.pt/2022/01/16/mundo/noticia/parlamento-frances-aprova-passe-vacinal-limita-vida-social-naovacinados-1992085. Ver também: https://eco.sapo.pt/2022/03/03/franca-anuncia-fim-da-mascara-e-passe-de-vacina-a-partir-de-14-de-marco/ (19.7.2022).

direitos fundamentais[203], tais como o direito à integridade física (art. 25), o direito ao livre desenvolvimento da personalidade (art. 26, n. 1) e, em alguns casos, o direito à liberdade de consciência e de religião (art. 41).

13. A PERSPECTIVA JURÍDICO-CONSTITUCIONAL DA VACINAÇÃO OBRIGATÓRIA

Considerando a discussão em torno da hesitação ou recusa vacinal, é preciso averiguar em que termos a defesa da saúde pública pode justificar a imposição da vacinação obrigatória (e a inevitável restrição a outros direitos fundamentais).

Pois bem. Não resta dúvida de que a questão é muito polémica, a começar pelo fato de que imposição da vacinação poder atentar contra o livre desenvolvimento da personalidade, a liberdade individual de decidir por si mesmo se irá ou não ser vacinado. Nas palavras de João Leal Amado, "A liberdade de cada pessoa, de cada trabalhador, implica, inevitavelmente, isso mesmo: a liberdade de, por vezes, acabar por tomar decisões estúpidas, idiotas ou imbecis. Essa liberdade deve ser ciosamente salvaguardada, tanto mais ciosamente quanto ela se manifeste em ações, omissões e opiniões das quais discordamos, até ao momento em que entre em choque com a liberdade alheia, até ao momento em que essa decisão individual colida com os direitos de outrem ou com o interesse coletivo"[204].

De fato, como sabemos, não há direitos absolutos, a liberdade de uns termina onde começa a liberdade alheia. A própria Constituição estabelece os parâmetros para a restrição a direitos e liberdades fundamentais nos números 2 e 3 do art. 18.

Com efeito, apesar de a CRP não se referir expressamente ao princípio da proibição do excesso ou da proporcionalidade em sentido lato, ele é extraído do disposto no n. 2 do seu art. 18 e o seu alcance enquanto tal foi acolhido pela jurisprudência constitucional, que a ele se recorre para a resolução de conflitos desde os mais simples até aqueles mais complexos, traduzindo-se, portanto, como um fundamental instrumento de controle da actuação restritiva das liberdades individuais.

A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição[205], com vistas a salvaguardar outros

---

[203] Aquilino Paulo Antunes – Vacinas para a Covid-19: aspectos para reflexão. *Revista da Faculdade de Direito da Universidade de Lisboa*. Vol. 61, nº 2 (2020), p. 150.

[204] João Leal Amado – Vacinação obrigatória para quem trabalha? *Observatório Almedina*. 12 Jan. 2022. Disponível em: https://observatorio.almedina.net/index.php/2022/01/12/vacinacao-obrigatoria-para-quem-trabalha/ (7.3.2022).

[205] No Acórdão nº 155/2007, o Tribunal Constitucional destacou que "uma primeira leitura deste preceito poderia sugerir que aqueles direitos fundamentais, como é o caso de

direitos ou interesses constitucionalmente protegidos, devendo a restrição ser adequada, necessária e proporcional[206]. Os conflitos devem ser resolvidos com base em critérios de concordância prática, amparada no princípio da proporcionalidade, significando dizer que as decisões devem ser ponderadas caso a caso. Além disso, as leis restritivas de direitos, liberdades e garantias têm de revestir carácter geral e abstrato e não podem ter efeito retroativo nem diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais[207]. Assim, caso se pretenda tornar obrigatória a vacinação, por se tratar de matéria relativa a direitos, liberdades e garantias, além da aprovação ou autorização por diploma parlamentar (alínea *b*) do n. 1 do art. 165 da CRP, a medida haverá de passar também no teste da proporcionalidade consagrado no n. 2 do artigo 18 da Lei Fundamental[208].

Consoante ensinamentos de Canotilho e Vital Moreira, a restrição ao exercício de direitos, liberdades e garantias deverá respeitar, cumulativamente, as seguintes condições: *a)* que a restrição seja expressamente admitida pela Constituição[209]; *b)* que a restrição vise salvaguardar outro direito ou interesse constitucionalmente protegido, não podendo o sacrifício ser desmotivado ou arbitrário; *c)* que a restrição exigida para essa salvaguarda seja apta para o efeito e se limite à medida necessária para alcançar esse objetivo; *d)* que a restrição não aniquile o direito em causa atingindo o conteúdo essencial do respectivo preceito[210].

O princípio da proibição do excesso ou da proporcionalidade em sentido lato é subdivido em três subprincípios, quais sejam o princípio da adequação (ou da idoneidade), o princípio da necessidade (ou da indispensabilidade)

alguns dos que agora estão em causa (por exemplo, o direito à integridade física), para os quais a própria Constituição não prevê expressamente a possibilidade de restrições legais, seriam, pura e simplesmente, insusceptíveis de ser restringidos. O reconhecimento do carácter incomportável de uma tal leitura, designadamente do ponto de vista das suas consequências práticas, levou, contudo, ao desenvolvimento jurisprudencial e doutrinário de uma multiplicidade de soluções - como o recurso, entre outros, ao artigo 29ºda Declaração Universal dos Direitos do Homem, às autorizações "indirectas ou tácitas" de restrições, às ideias de "limites imanentes", de "limites constitucionais não escritos", de "limites intrínsecos", de "restrições implícitas", de "limites instrumentais" - que, de uma ou outra forma, têm afastado aquela conclusão.

206 Nº 2 do Art. 18º da CRP.

207 Nº 3 do Art. 18º da CRP.

208 Aquilino Paulo Antunes – Vacinas para a Covid-19: aspectos para reflexão. *Revista da Faculdade de Direito da Universidade de Lisboa*. Vol. 61, nº 2 (2020), p. 150.

209 "Consideração particular neste contexto exige o caso em que a lei pretende revelar limites que não se encontram previstos ou mencionados na Constituição, mas que hajam de entender-se implicitamente decorrentes do seu texto, designadamente por efeito de colisão de direitos: são as restrições não expressamente autorizadas pela Constituição, tradicionalmente conhecidas como limites imanentes." J.J. Gomes Canotilho; Vital Moreira. *Constituição da República Portuguesa Anotada*. Vol. I. 4ª ed. Coimbra: Coimbra Editora, 2007. p. 389.

210 J.J. Gomes Canotilho; Vital Moreira. *Constituição da República Portuguesa Anotada*. Vol. I. 4ª ed. Coimbra: Coimbra Editora, 2007. p. 388.

e, finalmente, o princípio da proporcionalidade em sentido restrito. Jorge Reis Novais, de maneira bastante didática, sintetiza tais subprincípios da seguinte forma:

> Na sua utilização mais comum, ao princípio da idoneidade é atribuído o sentido de exigir que as medidas restritivas em causa sejam aptas a realizar o fim visado com a restrição ou contribuam para o alcançar; ao princípio da indispensabilidade ou da necessidade o sentido de que, de todos os meios idóneos disponíveis e igualmente aptos a prosseguir o fim visado com a restrição, se deve escolher o meio que produza efeitos menos restritivos; por sua vez, o princípio da proporcionalidade em sentido restrito respeitaria à justa medida ou a relação de adequação entre os bens e interesses em colisão ou, mais especificamente, entre o sacrifício imposto pela restrição e o benefício por ela prosseguido.[211]

O Estado de Direito rechaça qualquer afetação a direito fundamental ou restrição a liberdade que seja excessiva, ou seja, que vá para além do estritamente necessário ou adequado. Parafraseando o autor acima citado, a dignidade da pessoa humana e o direito fundamental ao desenvolvimento da personalidade ou, noutra perspectiva, a liberdade geral de acção nele fundada, confere aos cidadãos, num Estado de Direito, uma pretensão jurídico-constitucionalmente protegida de não terem a sua liberdade individual negativamente afectada a não ser quando tal seja estrita e impreterivelmente exigido pela prossecução, por parte dos poderes públicos, de outros valores dignos de protecção jurídica[212].

À luz do princípio da adequação, deve-se perguntar se o meio é adequado para a prossecução do fim visado pela lei. Diz respeito exclusivamente à relação de causa-efeito entre meio e fim, à aptidão de um meio para atingir um fim. Assim, nesta fase prévia, a medida restritiva só será liminarmente invalidada por inidoneidade ou inaptidão quando os seus efeitos se revelem indiferentes, inócuos ou até negativos tomando como parâmetro a aproximação do fim visado com a restrição[213]. Como bem define Vitalino Canas, meio adequado é aquele que é intrinsecamente capaz de desencadear ou causar efeitos materiais positivos de promoção de bens, interesses ou valores visados pelo legislador, sendo requerida apenas uma eficiência mínima, sem a realização de qualquer juízo de ponderação[214]. Ademais, tanto os fins prosseguidos como os meios empregados hão de ser legítimos. Para elucidar a questão, pode-se pensar numa situação em que o fim perseguido é, em si, legítimo (p. ex., a salvaguarda da segurança nacional), porém os

---

211 Jorge Reis Novais – *Os princípios constitucionais estruturantes da República Portuguesa*. Coimbra: Coimbra Editora, 2004. p. 162-163.

212 Jorge Reis Novais – *Os princípios constitucionais estruturantes da República Portuguesa*. Coimbra: Coimbra Editora, 2004. p. 163-164.

213 *Ibid.*, 168.

214 Vitalino Canas – *O princípio da proibição do excesso na conformação e no controlo de atos legislativos*. Coimbra: Almedina, 2017. p. 1163.

meios empregados são ilegítimos (p. ex., a prática de tortura). Seja como for, todos e quaisquer fins ou meios que atentem contra a dignidade da pessoa humana não encontram guarida no ordenamento jurídico português.

À luz do princípio da necessidade, deve-se questionar se existe outra forma menos gravosa com a mesma eficácia. Consoante Vitalino Canas, a necessidade seria centro nevrálgico da proibição do excesso, sendo o meio elegível considerado necessário quando, entre os disponíveis, não há alternativa menos interferente com intensidade de satisfação pelo menos aproximadamente igual. Com vistas a ilustrar a aplicação prática do princípio, para exprimir a ideia de que se deve evitar danos desnecessários, não exigíveis pela realização do fim, Jorge Reis Novais faz referência à fórmula consagrada de Fleiner: *não se deve utilizar um canhão para atirar a pardais*[215].

Finalmente, à luz do princípio da proporcionalidade em sentido estrito, deve-se colocar na balança o custo-benefício de determinada restrição, ou seja, cumpre observar se houve mais benefícios do que prejuízos. Trata-se, essencialmente, de questionar sobre a adequação (proporção) de uma relação entre dois termos ou duas grandezas variáveis e comparáveis: de um lado, a importância ou premência do fim que se pretende alcançar com a medida restritiva e, do outro, a gravidade do sacrifício que se impõe com a restrição[216]. Segundo Vitalino Canas, é neste âmbito que se valoram e se contrapesam os efeitos positivos referentes à satisfação de bens, interesses ou valores e os efeitos negativos de interferência em bens, interesses ou valores com aqueles colidentes, devendo-se tomar como parâmetro de comparação o impacto que os efeitos produzem sobre o ambiente geral de liberdade[217] - considerando-se que a CRP está assentada na liberdade.

A coexistência equilibrada dos direitos fundamentais é tarefa árdua. Situações como a da atual pandemia podem envolver conflitos entre diferentes direitos e liberdades fundamentais, devendo recorrer-se à ponderação para chegar-se às melhores soluções jurídicas, isto é, balanceando-se os diferentes interesses em jogo, consoante as circunstâncias fáticas do caso concreto, e de modo que todos os direitos envolvidos alcancem a máxima efetividade possível diante de tais circunstâncias[218].

---

215 Jorge Reis Novais – Os princípios constitucionais estruturantes da República Portuguesa. Coimbra: Coimbra Editora, 2004. p. 171.

216 Jorge Reis Novais – Os princípios constitucionais estruturantes da República Portuguesa. Coimbra: Coimbra Editora, 2004. p. 178.

217 Vitalino Canas – *O princípio da proibição do excesso na conformação e no controlo de atos legislativos*. Coimbra: Almedina, 2017. p. 1164.

218 Jessica Andrade Modesto; Marcos Erhadt Júnior – Danos colaterais em tempos de pandemia: preocupaçãoes quanto ao uso dos dados pssoais no combate à covid-19. In ROdrigo Nóbrega Farias; Igor De Lucena Mascarenhas (orgs.) – *COVID-19: saúde, judicialização e pandemia*. Curitiba: Juruá Editora Juruá, 2020, p. 154.

O princípio da proporcionalidade foi especialmente analisado pelo TJUE no acordão Schecke[219]. Neste acórdão, o TJUE concluiu que "o princípio da proporcionalidade faz parte dos princípios gerais do direito da União e exige que os meios postos em prática por um acto da União sejam aptos a realizar o objectivo prosseguido e não vão além do que é necessário para o alcançar" e que "as derrogações à protecção dos dados pessoais e as suas limitações devem ocorrer na estrita medida do necessário". Ou seja, de acordo com os limites impostos pelo princípio da proporcionalidade, uma medida será necessária quando as finalidades prosseguidas não puderem ser alcançadas através de medidas menos restritivas do direito dos titulares no que respeita à sua vida privada, em geral, e à proteção dos seus dados pessoais, em particular. É fundamental que haja uma ponderação equilibrada entre os interesses públicos e de terceiros, por um lado, e os direitos fundamentais dos titulares, por outro.

Com base na atual e concreta ameaça da saúde pública e à luz do princípio da proporcionalidade, concordamos com aqueles que defendem que antes de tornar obrigatória a vacinação se deverá recorrer a recursos menos intrusivos de combate à pandemia, tais como campanhas de informação e conscientização em relação à vacinação, obrigatoriedade da utilização das máscaras de proteção, ventilação dos ambientes, testagens, distanciamento entre as pessoas, teletrabalho sempre que possível, redução do número de pessoas em eventos, fortalecimento da qualidade dos serviços de saúde, etc[220].

Obviamente, o que aqui se defende assenta no pressuposto fático de que a vacinação disponível contra COVID-19 possui eficácia comprovada para neutralizar ou minimizar os riscos de contágio do vírus e que há recursos alternativos disponíveis, tais como os testes de detecção (os testes PCR e antígeno), que sugerem ou, pelo menos, possibilitam propor a existência de alternativa capaz de garantir com semelhante nível de segurança que a pessoa não represente risco de contágio para os demais[221].

Em Portugal, país no qual houve uma adesão voluntária massiva à vacinação, esta continua a ser apenas recomendada[222].

---

219 Vide Processos nºs C 92/09 e C 93/09.

220 Disponível em: https://www.sapo.pt/opiniao/artigos/vacinacao-obrigatoria-em-portugal-e-legal (8.4.2022).

221 César Cierco Seira – La vacuna-condición o el pasaporte de vacunación y su eventual encajeen un marco general de vacunación recomendada contra la COVID-19. *National Library of Medicine*. Vol. 22, nº 2 (Maio/Ago 2021), p. 82-88.

222 "Em todo o mundo, as posições dos governos relativamente a tornar obrigatória a toma da vacina divergem. E se em Portugal a vacinação é voluntária, pela Europa há alguns setores em que é obrigatório tomar a vacina, como é o caso dos profissionais de saúde ou dos trabalhadores em lares." Disponível em: https://eco.sapo.pt/2021/07/14/nestes-paises-a-vacina-contra-a-covid-e-obrigatoria-para-alguns-setores/ (8.4.2022). Ver também: https://www.dn.pt/sociedade/costa-portugal-entende-que-nao-deve-haver-vacinacao-obrigatoria-14393060.html (8.4.2022).

Porém, há que se registrar que essa solução poderá ser reequacionada caso a realidade venha a alterar-se, por exemplo, se porventura houver um aumento drástico da mortalidade diante do agravamento da situação pandêmica[223]. Como bem salientam Rui Guimarães e outros juristas, "a existência e interpretação do Direito tem que ser feita à luz da realidade a que deve ser aplicado; caso contrário, temos uma conceção delirante, alheada da realidade, do próprio Direito, o que significa a negação da sua própria razão de ser."[224].

Seja como for, o estabelecimento da vacinação obrigatória deve passar pelo pertinente juízo da proporcionalidade, devendo-se levar em consideração diferentes fatores, entre eles a efetividade das vacinas e os riscos diretos ou potenciais para quem as recebe[225].

13.1. A OBJEÇÃO DE CONSCIÊNCIA FACE À IMPOSIÇÃO DA VACINAÇÃO

O direito fundamental à objecção de consciência corresponde à posição subjectiva constante do Direito Constitucional (artigos 41, n. 6 e 276, n. 4), pela qual se isenta de quaisquer sanções o incumprimento de um dever jurídico específico, por razões relacionadas com as convicções do respectivo titular, desde que realizado de um modo individual, pacífico e privado[226].

É a objeção de consciência um mecanismo de defesa constitucionalmente consagrado[227] que visa salvaguardar a dignidade da pessoa humana quando esta seja posta em causa por uma determinada conduta[228]. Enquanto manifestação da dignidade da pessoa humana e da liberdade de consciência, traduz-se na recusa em cumprir um dever jurídico-positivo[229] fundada nos

---

223 Disponível em: https://www.sapo.pt/opiniao/artigos/vacinacao-obrigatoria-em-portugal-e-legal (8.4.2022).

224 rui GuimarãeS [et al.] – Acesso e reutilização de registos clínicos para fins de investigação no âmbito da pandemia por COVID-19. *Revista do Ministério Público*. Vol. 163 (Jul./Set., 2020), p. 203-226.

225 Iván Antonio Rodríguez Cardo – *Prohibición de discriminación en el trabajo por razón de covid*. Pamplona: Aranzadi–Thomson Reuters, 2021, p. 55.

226 Jorge Bacelar Gouveia – Objecção de consciência (direito fundamental à). In José Pedro Fernandes; Afonso Rodrigues Queiró (coords.) – *Dicionário Jurídico da Administração Pública*. Lisboa. Vol. 6 (1994), p. 165 e ss.

227 O nº 2 do art. 10 da *Carta dos Direitos Fundamentais da União Europeia* remete para as legislações nacionais o âmbito de exercício do direito. Na Constituição portuguesa, este direito está expressamente previsto, em termos gerais, no nº 6 do art. 41, e, em termos especiais, quanto ao serviço militar, no nº 4 do art. 276.

228 J.J. Gomes Canotilho; Vital Moreira – *Constituição da República Portuguesa Anotada*. Vol. I. 4ª ed. Coimbra: Coimbra Editora, 2007. p. 609-610.

229 Não se confunde, porém, com a desobediência ao direito (em sentido estrito), enquanto "simples incumprimento de um dever jurídico", não motivado por razões de consciência e que desencadeia a aplicação de sanções, como nota: Jorge Bacelar GOUVEIA – Objecção de consciência (direito fundamental à). In José Pedro Fernandes; Afonso Rodrigues Queiró (coords.) – *Dicionário Jurídico da Administração Pública*. Lisboa. Vol. 6 (1994), p. 165 e ss.

ditames da consciência do indivíduo, os quais abrangem razões (estritamente) morais, humanísticas, religiosas, filosóficas, sociológicas ou ideológicas - mas, em todo o caso, um juízo moral, radicado na consciência singular[230], sem poder ser perseguido, privado de direitos ou isento de obrigações ou deveres cívicos.

Em decorrência do carácter multicultural das sociedades actuais (resultante, em certa medida, dos fluxos migratórios)[231], o instituto expandiu-se para além do domínio tradicional do serviço militar obrigatório (art. 276, n. 4, CRP), podendo ser invocado em quaisquer situações em que esteja em causa razões de consciência (morais, filosóficas, etc.)[232], fundadas em propósito firme, devidamente interiorizado, não de uma mera opinião; essa ideia, sendo convicta, deve impor-se à pessoa como algo a que ela está adstrita e que não pode deixar de dar seguimento[233].

Porém, como todo direito fundamental, o direito à objeção de consciência pode ser limitado ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos (art. 18, n. 2, CRP).

Miremos na realidade: em meio a pandemia do coronavírus – que já causou a morte de milhões de pessoas -, determinado empregado de uma empresa, invocando o direito à objeção de consciência, recusa a vacinar-se. A colisão de direitos fundamentais ocorre porque de um lado está a liberdade fundamental individual do empregado que se recusa a vacinar, pautado em ditames de consciência individual, e do outro está o valor constitucional coletivo, exercido pelo empregador, em nome do interesse de toda a sociedade de manter a preservação da vida dos cidadãos trabalhadores.

Em situações de difícil solução como a que fora exposta acima deve-se realizar a ponderação, em concreto, entre as liberdades e direitos fundamentais em conflito, recorrendo-se ao princípio da concordância prática estampado no n. 2 do art. 18, CRP.

Primeiramente, faz-se mister averiguar se a situação comporta, de fato, uma real ameaça à coletividade. Para tanto, deve-se investigar o nível de disseminação da pandemia na comunidade no momento da avaliação e as condições em que o trabalho é prestado, tais como se o funcionário trabalha sozinho ou com outras pessoas, interno ou externamente, se o local de trabalho possui ventilação adequada, a frequência e a duração da interação direta que o funcionário normalmente terá com outros funcionários e terceiros, o número de pessoas parcial ou totalmente vacinadas no ambiente de trabalho, se ou-

---

230 Paulo Pulido Adragão; Anabela Costa Leão – O Direito à Objecção de Consciência por parte do Chefe de Estado, em Questão. O caso da recusa de promulgação de actos legislativos por motivo de consciência. In AA. VV – *Estudos em Homenagem ao Professor Doutor Jorge Miranda*. Coimbra: Coimbra Editora. Vol. 3 (2012).

231 Idem.

232 J.J. Gomes Canotilho; Vital Moreira – *Op. cit.*, p. 616.

233 Jorge Bacelar Gouveia – *Op. cit.*, p. 165 e ss.

tros funcionários estão usando máscaras ou passando por testes de triagem de rotina, se há espaço disponível para o distanciamento social etc[234].

Constatada a existência de ameaça real à coletividade e recusando-se o funcionário a atender a requisição da vacinação por causa de uma crença religiosa realmente sincera - não sendo suficiente uma simples crença "anti-vax", como chama atenção Margaret R. Kurlinski[235], o impasse está gerado[236].

Ante tal situação, compreendo que a solução que melhor acomoda os interesses de ambos os lados é aquela que prevê que o empregador envide esforços para proporcionar acomodações razoáveis para o empregado que se recusa a ser vacinado contra o COVID-19. Nesse contexto, poderá o empregador exigir o uso contínuo de equipamentos de proteção individual, assegurar o trabalho à distância de colegas de trabalho ou não funcionários, o trabalho em um turno modificado, a realização de testes periódicos para COVID-19 ou até mesmo oportunizar o teletrabalho ou a reatribuição, desde que, obviamente, tais medidas não representem uma dificuldade indevida ou excessiva para o seu empreendimento[237].

Assim, verificada a existência de real ameaça à coletividade, porém havendo alternativas razoáveis e disponíveis ao empregador que eliminem ou reduzam o risco da ameaça direta das pessoas não vacinadas, considero justificado o acolhimento da objeção de consciência à vacinação invocada pelo empregado[238].

Em contrapartida, em não existindo alternativas razoáveis e disponíveis que possam ser implementadas pelo empregador, entendo que a recusa individual à vacinação, sob uma reserva de consciência, quando confrontado com um interesse fundamental coletivo, quando há risco à saúde da coletividade, não deve prevalecer, especialmente em tempos de pandemia[239].

Conforme se percebe, o grande desafio será buscar compatibilizar a proteção coletiva com a liberdade de consciência individual. Seja como for, a objeção de consciência não pode ser examinada de maneira isolada: trata-se de atingir soluções que contemplem o respeito pelas liberdades indivi-

---

234 What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws. Disponível em: https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws.

235 Margaret R. Kurlinski – COVID-19: An Employer's Role in Vaccination. *Corporate Counsel*. Vol. 35, nº 1 (2021), p. 4-7.

236 *Ibid.*, p. 4-7.

237 What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws. Disponível em: https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws (15.3.2022).

238 Idem.

239 A Suprema Corte do Brasil (STF), na ADI nº 6586, 6587 e no Recurso Extraordinário com Agravo (ARE) nº 1267879, firmou o entendimento de que o interesse coletivo prevalece sobre os individuais, quando se trata de erradicar a doença da COVID-19, a despeito da Carta assegurar e proteger os direitos dos trabalhadores de índoles moral, espiritual e pessoal.

duais, a proteção do interesse comum e a defesa dos direitos fundamentais. Em nenhum caso, a sua invocação poderá ser um recurso para obstruir ou limitar direitos[240].

14. É POSSÍVEL EXIGIR "PASSAPORTE VACINAL" NO AMBIENTE DE TRABALHO?

Quando se coloca a questão da legitimidade de um empregador aceder a informações médicas, mais especificamente sobre o *status* da vacinação dos seus funcionários no âmbito da COVID-19, o que se faz é uma ponderação dos bens jurídicos e interesses em causa.

Enquanto a testagem nos locais de trabalho parece ser consensual entre empresas e trabalhadores, o conhecimento acerca do *status* de vacinação ou a exigência da vacinação para adentrar nas instalações da empresa ou até mesmo aceder aos postos de trabalho continua a ser assunto polêmico[241], conforme será exposto abaixo, mormente porque constitui, em última medida, numa forma indirecta de impor a vacinação obrigatória.

14.1. DA IMPOSSIBILIDADE DE EXIGÊNCIA DA VACINAÇÃO SEM SUPORTE LEGISLATIVO

Considerando que a vacinação contra a SARS-CoV-2 não tem, pelo menos não em Portugal, cariz obrigatório, há quem defenda que enquanto não houver alteração legislativa, não estariam os empregadores autorizados a exigir dos candidatos a emprego e/ou aos seus trabalhadores prova da imunização como condição de acesso às suas instalações ou ao posto de trabalho[242], posto que tal exigência seria, no final das contas, uma maneira indirecta de tornar a vacinação, que até o presente momento é apenas recomendada, em obrigatória[243].

Essa defesa repousa no fato de que a restrição a direitos fundamentais só poderia ser operada por lei da Assembleia da República ou decreto-lei

---

240 Gabriela Irrazábal; Laura Belli; María Eugenia Funes – Direito à saúde *versus* objeção de consciência na Argentina. *Revista Bioética*. Brasília. Vol. 27, nº 4 (Out./Dez. 2019), p. 728-738. Disponível em: https://www.scielo.br/j/bioet/a/QsxNzMGKgRwsNpTz5KPmccQ/?lang=pt&format=pdf (18.5.2022).

241 Disponível em: https://www.jornaldenegocios.pt/economia/detalhe/patroes-admitem-vacinacao-obrigatoria-dos-trabalhadores (15.3.2022).

242 Disponível em: https://abreuadvogados.com/conhecimento/publicacoes/help-desk-covid-19/helpdesk-covid/poderes-de-controlo-do-empregador-para-a-vacinacao-e-outras-medidas-de-prevencao-da-doenca-covid-19/ (15.3.2022).

243 Aquilino Paulo Antunes – Vacinas para a Covid-19: aspectos para reflexão. *Revista da Faculdade de Direito da Universidade de Lisboa*. Vol. 61, nº 2 (2020), p. 150.

autorizado do Governo (alínea *b)* do n. 1 do art. 165 da CRP)[244] e, por consequência, o juízo de ponderação quanto à obrigatoriedade da vacinação deveria ser feito pelos órgãos de soberania constitucionalmente competentes, e não por uma entidade privada, desprovida de poderes públicos, como é a entidade empregadora, no seio de uma qualquer empresa[245].

Neste sentido, não poderia o empregador, pautado num pretenso poder de direção ou até no alegado cumprimento dos seus deveres em matéria de segurança e saúde dos trabalhadores, substituir-se ao Poder Público e tornar a vacinação contra COVID-19 obrigatória, por mera decisão unilateral, para toda e qualquer situação, nomeadamente em situações que aparentemente não indicam qualquer risco adicional no exercício das atividades[246].

Assim, segundo esta corrente, enquanto não houver previsão legal específica[247] exigindo o passaporte vacinal para o exercício de atividades laborais, não poderá o empregador, imiscuindo-se na função dos poderes públicos competentes, impor o comprovante de vacinação a seus funcionários[248].

---

244 "Essa reserva de competência legislativa parlamentar – e implicitamente reserva material de lei – estende-se a todos os aspectos do regime dos direitos, liberdades e garantia e não apenas ao caso das restrições, pois a al. b do art. 165º-1 não discrimina." J.J. Gomes Canotilho; Vital Moreira. *Constituição da República Portuguesa Anotada*. Vol. I. 4ª ed. Coimbra: Coimbra Editora, 2007. p. 396.

245 Gerou grande repercussão o anúncio por parte do Citigroup, uma das maiores entidades bancárias dos Estados Unidos, de que iria despedir os funcionários não vacinados contra a covid-19 que não apresentassem uma justificação. Disponível em: https://www.dn.pt/internacional/citigroup-vai-despedir-funcionarios-nao-vacinados--nos-eua-14472383.html (7.3.2022).

246 João Leal Amado – Vacinação obrigatória para quem trabalha? *Observatório Almedina*. 12 Jan. 2022. Disponível em: https://observatorio.almedina.net/index.php/2022/01/12/vacinacao-obrigatoria-para-quem-trabalha/ (7.3.2022).

247 "In the European Union, several member states—such as France, Poland, Latvia and Bulgaria—have introduced policies of mandatory vaccination for certain diseases (e.g. measles), but none have applied this to COVID- 19 vaccination. Italy was the first European country to make COVID vaccination mandatory for all healthcare workers, after discovering outbreaks inside hospitals related to medical staff who had declined the vaccine. In the UK, there are no compulsory vaccines and the government has stated that it has no intention of changing the law in this area despite COVID-19. Indeed, a policy of mandatory vaccination could infringe some rights of employees, as expressed by the European Convention on Human Rights, such as right to liberty and security (article 5), right to respect for private and family life (article 8), freedom of thought, conscience and religion (article 9) and prohibition of discrimination (article 14)." Michele Augusto Riva; Maria Emilia Paladino; Andrea Paleari; Michael Belingheri – Workplace COVID-19 vaccination, challenges and opportunities. *Occupational Medicine*. England: Oxford. Vol. 72, nº 4 (Maio 2022), p. 235-237.

248 Disponível em: https://observatorio.almedina.net/index.php/2022/01/12/vacinacao-obrigatoria-para-quem-trabalha/ (7.3.2022).

14.2. DA OBRIGATORIEDADE DA VACINAÇÃO COMO COROLÁRIO DO PODER DIRETIVO DO EMPREGADOR

Em sentido diametralmente oposto[249], há quem defenda de maneira mais taxativa que do mesmo modo que a entidade patronal pode fixar o teletrabalho como obrigatório para todos os trabalhadores, também poderá proibir ou restringir o acesso de terceiros, de acordo com determinadas regras, designadamente pela detenção de Certificado COVID, por ser a empresa um edifício privado[250].

Este posicionamento encontra amparo no poder de direção consagrado pelo artigo 97, CT, que faculta ao empregador estabelecer os termos em que o trabalho deve ser prestado, dentro dos limites decorrentes do contrato e das normas que o regem. O empregador goza de uma espécie de poder geral de comando, cabendo-lhe determinar a concreta função a ser exercida pelo trabalhador, o poder de conformar a prestação laboral e ainda poderes de vigilância e controlo acerca da atividade desenvolvida pelo trabalhador durante o pacto laboral[251].

Não se pode ignorar o fato de que uma força de trabalho mais vacinada pode implicar a redução dos custos do local de trabalho, uma vez que os trabalhadores vacinados terão menos chances de contrair de forma grave o vírus COVID-19 e consequentemente o empregador terá que despender menos com ausências ou perda de produtividade[252].

---

249 "Private employers and educational institutions have issued vaccine mandates.47 Decisional privacy is less of a legal issue in these established relationships because individuals lose some privacy protections to receive the benefits of employment or a formal education. In many contexts employees and students must submit themselves to drug testing as a condition of their employment or education, thereby limiting the number of otherwise legal substances they might consume. Employees and students might choose to limit their communications because technology use policies grant employers and schools access to electronic communications that would be considered private in other contexts. In the same vein, nothing under federal law prevents "an employer from requiring all employees physically entering the workplace to be vaccinated for COVID-19." David SELLA-VILLA – The COVID-19 Pandemic One Year On: Finding Balance Between Privacy and Public Health. *The Business Lawyer*. Vol. 77 (Ago 2021).

250 Disponível em: https://portal.oa.pt/comunicacao/imprensa/2021/06/29/foi-barrado-na-sua-empresa-por-nao-estar-vacinado-lei-nao-permite-mas-ha-excecoes/ (10.3.2022).

251 João Leal Amado. Contrato de Trabalho noções básicas. Almedina, 2019, 3ª edição, p. 204.

252 "A mandatory vaccination approach also makes it more likely that a business can open and stay open. Even if there are no medical consequences, a single positive COVID-19 test can lead an employer to fully stop operations, particularly in industries like dining and hospitality. A highly vaccinated workplace reduces the likelihood of such stoppages. At the same time, high vaccination rates can accelerate a "return to normal" by making it safer for the workforce to return to the office or otherwise resume normal operations, and by creating a safer environment for customers." Jessica Brown; Lauren J. Elliot; Daniel Rauch – An employer playbook for the covid "vaccine wars": strategies and considerations for workplace vaccination policies. *Practical Lawyer*. Vol. 67, nº 1 (2021), p. 20-30.

Seguindo esta linha de raciocínio, cogita-se, inclusive, de uma eventual responsabilização dos empregadores[253], na medida em que a permissão de acesso de indivíduos não vacinados às suas instalações pode representar, em última medida, um risco de contaminação dos demais que compartilham do mesmo ambiente[254].

A exigência de prova da imunização dos trabalhadores dar-se-ia com base nas alíneas *h)* e *i)* do artigo 9, n. 2, RGPD (por ser necessária para efeitos de medicina preventiva ou do trabalho ou por motivo de interesse público no domínio da saúde pública), na medida em que incumbe ao empregador garantir a prestação do trabalho em condições de higiene, segurança e saúde e a exigência da vacinação é considerada medida que visa à contenção da pandemia, ao que acresce o próprio considerando 46, RGPD, que prevê a necessidade de tratamento desta categoria se for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana". Tendo em vista que a pandemia de COVID-19 provocou uma crise sanitária de natureza e escala sem precedentes, não há como negar que a luta contra a COVID-19 traduz-se como um interesse público importante, sendo, inclusive, reconhecida como tal pelo Comité Europeu para a Proteção de Dados (CEPD)[255].

Com base em tais considerações, desde que não afronte a legislação existente, estaria o empregador autorizado a adotar uma política de vacinação obrigatória em toda e qualquer situação[256]. Seja como for, não há

---

253 "Across the United States, lawsuits for wrongful death, negligence, and retaliation are being filed against businesses for their failure to protect employees and the public from the known dangers of COVID-19.1 Tyson Foods was sued for wrongful death by the widow of a Tyson employee who contracted COVID-19 five days after administering temperature checks for Tyson employees at a meatpacking plant. He died from COVID-19 two weeks later.2 A Trader Joe's employee filed a complaint with the National Labor Relations Board claiming he was terminated in retaliation for requesting greater COVID-19 protections from his employer.3 New York sued Amazon for disregarding health standards in Amazon warehouses.4 Colorado congressman Doug Lamborn was sued by a former employee who claims the congressman failed to implement any safety standards and as a result contributed to the spread of COVID-19 to his staff.s Most recently, following the death of four courthouse workers, the Superior Court of Los Angeles was fined more than $25,000.00 for COVID-19 safety violations." H. R. Falks – Covid-19 employer liability still unknown. *Court Review*. Vol. 57, nº 3, p. 164-171.

254 Jessica Brown; Lauren J. Elliot; Daniel Rauch – *Op. cit.*, p. 20-30.

255 Diretrizes 03/2020 sobre o tratamento de dados relativos à saúde para efeitos de investigação científica no contexto do surto de COVID-19. Adotadas em 21 de abril de 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_pt.pdf (7.7.2022).

256 RELATÓRIO DA COMISSÃO AO PARLAMENTO EUROPEU E O CONSELHO nos termos do art. 16º, nº 2, do Regulamento (UE) 2021/953 do Parlamento Europeu e do Conselho relativo a um quadro para a emissão, verificação e aceitação de certificados interoperáveis de vacinação, teste e recuperação contra a COVID-19 (UE Digital COVID Certificado) para facilitar

como ignorar que a falta de expressa previsão legislativa termina por travar a implementação de tal medida no âmbito das empresas, ante os receios que gravitam em torno da questão, a saber *i)* dúvidas em relação ao procedimento administrativo a ser seguido no caso, por exemplo, de serem suscitadas isenções quanto à vacinação obrigatória; *ii)* preocupações em torno da possibilidade de invasão da privacidade dos funcionários; *iii)* natureza impopular de tal uma política; e/ou *iv)* preocupações com relação à responsabilidade no caso de efeitos adversos por reação à vacina[257].

Na prática, até que a vacina contra COVID-19 seja tornada obrigatória pelos órgãos públicos competentes, a melhor estratégia continua a ser o diálogo e a conscientização com os funcionários da empresa, cabendo aos empregadores esclarecer as possíveis dúvidas sobre a segurança e a eficácia das vacinas[258].

14.3. DA POSSIBILIDADE DA EXIGÊNCIA DA VACINAÇÃO QUANDO PREEENCHIDO O REQUISITO DA NECESSIDADE

Como é cediço, constitui dever primordial do empregador zelar pela saúde e segurança de seus trabalhadores e prevenir riscos laborais. Diante desta perspectiva, incumbe-lhe adotar as recomendações das autoridades de saúde no que diz respeito ao combate da pandemia do COVID-19, notadamente as medidas de implementação do teletrabalho, o fornecimento de equipamento de proteção individual, a manutenção das distâncias de segurança e a realização de desinfeção e limpezas periódicas das instalações[259].

Para além das situações previstas na legislação em matéria de saúde e segurança no trabalho, o empregador não pode, por regra, segundo o artigo 19, CT, exigir do candidato a emprego ou a trabalhador a realização ou apresentação de testes ou exames médicos, de qualquer natureza, para comprovação das condições físicas ou psíquicas, para efeitos de admissão ou permanência no emprego. Em que pese o dispositivo referir-se apenas a testes e exames médicos, e não especificamente a certificados de vacinação, po-

a livre circulação durante a pandemia de COVID-19. Bruxelas, 15 Mar. 2022. Disponível em: https://www.europarl.europa.eu/doceo/document/A-9-2022-0138_PT.html (20.7.2022).

257 Pamela Abbate-Dattilo – Navigating the legal challenges of covid-19 vaccine policies in private employment: school vaccination laws provide roadmap. *Mitchell Hamline Law Review*. Vol. 47, nº 3 (2021), p. 1019.

258 "Communication on vaccine efficacy and safety should be open and honest, non-stigmatizing with frequent updates. Early data show that the vaccines may prevent transmission of COVID-19, so employees should understand that community protection and individual protection are dependent on all the population being immune/vaccinated." Michele Augusto Riva; Maria Emilia Paladino; Andrea Paleari; Michael Belingheri – Workplace COVID-19 vaccination, challenges and opportunities. *Occupational Medicine*. England: Oxford. Vol. 72, nº 4 (Maio 2022), p. 235-237. DOI: https://doi.org/10.1093/occmed/kqab080.

259 Disponível em: https://adcecija.pt/passaporte-de-imunidade-no-contexto-laboral/ (10.3.2022).

de-se interpretá-lo como contemplando todos os tipos de comprovativos, inclusive o comprovativo de vacinação[260]. O princípio geral é o mesmo, a proteção da esfera privada do empregado.

Porém, em algumas situações elencadas pela própria norma, comportam-se exceções, a saber: *i)* quando tiver por finalidade a protecção e segurança do trabalhador ou de terceiros ou *ii)* quando particulares exigências inerentes à actividade o justifiquem. Em todo o caso, a justificativa deverá ser fornecida ao candidato a emprego ou ao empregado por escrito e o empregador apenas será comunicado pelo médico responsável pelos testes e exames médicos se o trabalhador está ou não apto para desempenhar a actividade[261].

O debate assume contornos delicados quando se subordina o acesso ao mercado de trabalho à apresentação de um certificado de vacinação, uma vez que tal informação diz respeito a um dado sensível relativo à saúde do empregado e, como tal, pode afetar alguns outros direitos e liberdades fundamentais, tais como o direito ao livre desenvolvimento da personalidade, o direito à segurança no emprego[262] e o direito ao trabalho[263].

Com efeito, de um lado está a autodeterminação dos indivíduos, o livre desenvolvimento da personalidade humana, o direito ao trabalho, à liberdade e à privacidade das pessoas, e de outro está a saúde e o dever do empregador de garantir um ambiente de trabalho sadio e seguro para os seus empregados. Caberá ao aplicador do direito sopesar os bens e interesses em confronto no caso concreto e verificar se o objetivo porventura não poderia ser atingido através de outro meio menos intrusivo.

Como outrora já alertamos, apesar de serem inegáveis os benefícios da vacinação para a coletividade como um todo e até provocar um certo espanto a aversão de algumas pessoas à imunização, o debate está longe de ser tranquilo. O responsável pelo tratamento/empregador haverá de verificar com a máxima acuidade possível se a exigência da vacinação é, de fato, justificável.

Consoante pode-se extrair do n. 1 do art. 19, CT, a empresa não poderá exigir o comprovativo de vacinação com base em preocupações gerais de segurança e saúde no local de trabalho, tampouco por mera conveniência empresarial. Pelo contrário, será necessário que particulares características da atividade justifiquem tal exigência, devendo a empresa fornecer por escrito ao candidato a emprego ou trabalhador a respectiva fundamentação[264].

A obrigatoriedade da comprovação da vacinação contra a COVID-19 haverá de passar pelo teste da proporcionalidade. A depender do tipo de atividade

---

260 Disponível em: https://eco.sapo.pt/2021/08/28/sem-vacinacao-obrigatoria-lei-impede-exigencia-de-certificado-pelas-empresas/ (7.4.2022).

261 Art. 19 do Código do Trabalho.

262 Art. 53, CRP.

263 Art. 58, CRP.

264 Disponível em: https://eco.sapo.pt/2021/08/28/sem-vacinacao-obrigatoria-lei-impede-exigencia-de-certificado-pelas-empresas/ (7.7.2022).

desenvolvida e das condições em que o trabalho é prestado, a exigência do certificado de vacinação poderá ser considerada medida ilegítima e desproporcional, particularmente se o objetivo puder ser atingido por outra via menos intrusiva[265]. Por exemplo, a imposição da vacinação em postos de trabalho em que não há um contato próximo entre as pessoas muito provavelmente será considerada ilegítima, posto não haver um perigo significativo de propagação do vírus[266], além de que outras medidas menos restritivas podem ser suficientes para mitigar os riscos de infecção e propagação da COVID-19[267].

Em outras circunstâncias, entretanto, pode ser legítimo ou até recomendável que as empresas se cerquem de maiores cuidados e exijam de seus funcionários o referido certificado de vacinação. Aqui, podemos incluir os empregados que laboram em lares de idosos e nos domínios da prestação dos cuidados de saúde[268].Porém, como bem adverte César Cierco Seira, a generalização da vacinação não pode ser estabelecida por si só como o motivo que justifica a condição. A fundamentação deve se dar à luz da natureza da atividade condicionada e, portanto, do interesse sanitário em reduzir o risco de contágio em seu desenvolvimento. Não se trata, segundo o autor, de escolher as atividades mais cotidianas para condicionar a participação nelas ao fato de estar vacinado e, assim, promover a extensão da vacina em postos de controle estratégico. Há que se identificar quais as atividades especialmente arriscadas para que se possa justificar o aumento das precauções quanto ao risco de contágio da doença e a exigência da prova de vacinação. Trata-se de um exercício complexo, onde, além de se analisar a natureza da atividade e/ou profissão em questão, deve-se também observar as características intrínsecas, exposição ao contágio, nível de contato, etc[269].

Assim, entendemos que o parâmetro norteador para legitimar a imposição da vacinação contra a COVID-19 será a proporcionalidade. Atividades que não implicam um risco acrescido de contaminação, seja porque não há um contato excessivo entre os trabalhadores ou até com terceiros, seja porque o local de trabalho possui grande ventilação, devem se valer de outros meios menos intrusivos para evitar a propagação da doença. De outro lado,

---

265 João Carlos Carvalho Godinho – *A (re)discussão dos fundamentos da vacinação humana obrigatória*. Coimbra: Almedina, 2022. p. 55-56; Carla Amado Gomes – *Defesa da Saúde vs. Liberdade Individual*: casos da vida de um médico de saúde pública. Lisboa: Associação Acadêmica da Faculdade de Direito de Lisboa, 1999. p. 120-121.

266 Jessica Brown; Lauren J. Elliot; Daniel Rauch – An employer playbook for the covid "vaccine wars": strategies and considerations for workplace vaccination policies. *Practical Lawyer*. Vol. 67, nº 1 (2021), p. 20-30.

267 Lauren Chalaturnyk – Covid-19 vaccines in the workplace: employees. *LawNow*. Vol. 45, nº 5 (2021), p. 36-38.

268 Disponível em: https://adcecija.pt/passaporte-de-imunidade-no-contexto-laboral/ (10.3.2022).

269 César Cierco Seira – La vacuna-condición o el pasaporte de vacunación y su eventual encajeen un marco general de vacunación recomendada contra la COVID-19. *National Library of Medicine*. Vol. 22, nº 2 (Maio/Ago 2021), p. 82-88.

atividades que exigem um contato próximo e inevitável entre os trabalhadores e principalmente com pessoas vulneráveis estão legitimadas a pedir a prova de vacinação.

A propósito, o Tribunal Constitucional Federal da Alemanha teve a oportunidade de se pronunciar recentemente sobre o assunto, tendo decidido pelo indeferimento de Reclamação Constitucional questionando a obrigatoriedade de funcionários dos setores de saúde e assistência apresentarem comprovante de vacinação contra a COVID-19. Na ocasião, entendeu-se que apesar da grande intensidade da ingerência, os direitos e liberdades fundamentais dos profissionais que atuam nos setores de saúde e assistência devem recuar com vistas a proteger grupos vulneráveis de adoecer gravemente ou até morrer de COVID-19. Ressaltou-se que a obrigação de prova de vacinação é proporcional em sentido estrito para os profissionais dos setores de saúde e assistência, pois, devido à natureza de seu trabalho, estão regularmente em contato intenso e próximo com pessoas vulneráveis, o que torna o risco aumentado de transmissão representado por funcionários que não foram vacinados e não recuperados mais relevantes e leva a um aumento considerável da necessidade de proteção das pessoas vulneráveis[270].

Outro aspecto que merece atenção é a evolução da situação epidemiológica causada pela pandemia da doença COVID-19, que, pelo menos em Portugal, tem sido positiva. Medidas de limitação da esfera jurídica da liberdade individual que anteriormente se justificavam para fazer frente à pandemia agora podem ser consideradas desnecessárias ou desproporcionais[271].

Toda e qualquer medida adotada no que respeita à pandemia de COVID-19 não deve ir além do estritamente necessário para salvaguardar a saúde pública. As operações de tratamento dos dados pessoais serão consideradas legítimas e proporcionais sempre que o meio se revelar necessário para a satisfação de uma finalidade concreta[272], cumprindo ao aplicador do direito adotar, dentre as medidas adequadas à prossecução do fim a atingir, a medida menos restritiva possível para os direitos fundamentais[273].

Logo, com fulcro nos princípios da proporcionalidade e da concordância prática, dependendo da situação em concreto e da evolução da situação

---

270 BVerfG, Beschluss des Ersten Senats vom 27. April 2022 - 1 BvR 2649/21 -, Rn. 1-281. Disponível em: http://www.bverfg.de/e/rs20220427_1bvr264921.html (24.5.2022).

271 Ante a evolução positiva da situação epidemiológica causada pela pandemia da doença COVID-19, o art. 13-C do Decreto nº 10-A/2020, que até então previa a possibilidade de se realizar medições de temperatura corporal a trabalhadores para efeitos de acesso e permanência no local de trabalho, por motivos de proteção da saúde do próprio e de terceiros, foi revogado pelo art. 4º do Decreto-Lei nº 23-A/2022.

272 Disponível em: http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/ (22.3.2022).

273 Jorge Miranda – *Direitos Fundamentais*. 3ª ed. Coimbra: Almedina, 2020. p. 339.

epidemiológica, poderá o empregador exigir dos seus funcionários a apresentação de comprovante de imunização, porém, em todo o caso, deve atuar com a máxima cautela possível, atentando-se precisamente à finalidade e à correspondente base legal autorizativa para o tratamento dessa categoria especial de dados[274], particularmente porque o certificado de vacinação contém dados sensíveis relativos à saúde que devem ser protegidos devido à sua íntima ligação com a privacidade[275].

15. PROIBIÇÃO DE DISCRIMINAÇÃO NO TRABALHO EM RAZÃO DO *STATUS* DA VACINAÇÃO

O debate em torno da vacinação obrigatória e as decisões sobre contratação, manutenção ou extinção do contrato baseadas na imunidade – real ou suposta - demonstram que a COVID pode converter-se em fator de discriminação, em geral, e no contexto da relação laboral, em particular. Isso acontece porque a COVID não repercute apenas sobre os contagiados, mas também sobre as pessoas que permanecem saudáveis, na medida em que as políticas de combate à enfermidade são de ordem pública e supõem severas restrições aos direitos fundamentais de todas as pessoas[276].

De uma perspectiva econômica e organizacional, os empregadores têm um interesse legítimo de que o ambiente de trabalho esteja livre de COVID, uma vez que eventual surto no espaço de trabalho pode, em última instância, provocar a paralisação da atividade produtiva. De outro lado, a possibilidade de levar em consideração elementos que demonstrem que o empregado não apresenta risco de COVID, como eventual comprovação de vacinação, pode vulnerar alguns direitos e liberdades fundamentais dos trabalhadores[277].

A Constituição prevê que "todos têm direito a um ambiente de vida humano, sadio e ecologicamente equilibrado e o dever de o defender[278]" e que todos os trabalhadores, sem distinção de qualquer natureza, têm direito "a prestação do trabalho em condições de higiene, segurança e saúde[279]". Ainda, que os empregados possuem o direito de desenvolver as suas atividades laborais sob condições de segurança, incumbindo ao empregador garantir

---

274 Guia técnico, LGPD no ambiente laboral, imunização e testagem de empregados como medida de enfrentamento à Covid-19. Disponível em: https://comply4.tech/ebook/ (9.2.2022).

275 César Cierco Seira – La vacuna-condición o el pasaporte de vacunación y su eventual encajeen un marco general de vacunación recomendada contra la COVID-19. *National Library of Medicine*. Vol. 22, nº 2 (Maio/Ago 2021), p. 82-88.

276 Iván Antonio Rodríguez Cardo – *Prohibición de discriminación en el trabajo por razón de covid*. Pamplona: Aranzadi–Thomson Reuters, 2021, p. 18-28.

277 *Ibid.*, p. 29-30.

278 Art. 66, nº 1, CRP.

279 Art. 59, nº 1, al. *c)*, CRP.

"boas condições de trabalho, do ponto de vista físico e moral", "tendo em conta a protecção da segurança e saúde do trabalhador"[280].

As obrigações empresariais de prevenção de riscos laborais atuam num plano distinto das medidas de saúde pública, pois enquanto as primeiras pretendem proteger os trabalhadores enquanto tal, as últimas visam evitar a propagação da enfermidade de um modo geral e não exclusivamente no entorno laboral, sendo tal distinção importante para determinar o alcance das faculdades empresariais[281].

No âmbito da prevenção de riscos laborais, as faculdades empresariais são exercidas com a finalidade específica de diminuir o risco a que o trabalhador está exposto pela natureza do trabalho (*v.g.* pessoal sanitário), e não de proteger em abstrato a saúde do trabalhador. Não deve o empregador extrair das normas de saúde pública, que estão voltadas especificamente às autoridades públicas, a habilitação para a adoção de medidas de combate à pandemia de caráter geral[282].

Neste sentido, não é indene de dúvida a possibilidade de o empregador decidir, unilateralmente, submeter os seus empregados a exames médicos, sem ao menos uma adequada análise de proporcionalidade. Os direitos e liberdades fundamentais dos trabalhadores aparecem nesses casos como limites ao poder de direção no contexto da prevenção de riscos laborais. Por exemplo, o direito à privacidade e à integridade física impedem que o empregador realize exames médicos periódicos, inclusive diários, para verificar se os empregados contraíram a enfermidade, caso a atividade laboral em concreto não ofereça um risco específico de exposição a agentes biológicos determinados, como o coronavírus[283].

A incerteza aumenta quando o propósito é averiguar a repercussão laboral da vacinação, devido à potencialidade mais invasiva da medida. É por isso que alguns juristas defendem que a obrigatoriedade da vacinação deve ser imposta por lei, e não por vontade do empregador, pois pode produzir consequências de alto relevo sobre os direitos fundamentais. Segundo Iván Antonio Rodríguez Cardo, as normas de prevenção de riscos laborais criam obrigações relativas à vacinação apenas para o empregador, no sentido de oferecer essa possibilidade aos seus empregados, e unicamente em atividades com risco específico de exposição a agentes biológicos (*v.g.* pessoal sanitário). Conforme o autor, a COVID é um problema de saúde pública, uma enfermidade que não surgiu no contexto de uma atividade concreta, e, portanto, não ocupa prioritariamente o plano da prevenção de riscos laborais. Desse modo, eventual imposição deve partir das autoridades sanitárias, e

280 Art. 127, nº 1, CT.

281 Iván Antonio Rodríguez Cardo – *Prohibición de discriminación en el trabajo por razón de covid*. Pamplona: Aranzadi–Thomson Reuters, 2021, p. 33-35.

282 *Ibid.*, p. 35-48.

283 *Ibid.*, p. 35-48.

não de um empregador, sendo as sanções pela recusa aquelas previstas na norma, que, por certo, não permitirá a administração forçada da vacina, mas poderá contemplar sanções ou limitações para quem as recuse, em forma de multas ou restrições à mobilidade[284].

A par da imposição da vacinação, também há objeção quanto à possibilidade de o empregador indagar o candidato a emprego ou o trabalhador de aspectos relacionados à COVID, mormente porque esta é considerada uma enfermidade estigmatizadora e que é fonte de discriminação. Com efeito, o empregador tem o legítimo interesse de buscar os empregados mais aptos e que possam oferecer o melhor rendimento para o trabalho, contudo esse interesse empresarial por vezes pode colidir com os direitos e liberdades fundamentais dos trabalhadores. Esse panorama assume relevância no contexto da COVID, quando o empregador, para otimizar a sua atividade produtiva, pretenda saber se o trabalhador já superou a enfermidade ou se já foi vacinado contra a doença[285].

Incursões desta natureza podem ensejar práticas discriminatórias no contexto da relação laboral, cabendo ao poder empresarial ponderar o seu "legítimo interesse" com as liberdades individuais do trabalhador, particularmente o direito à privacidade e o direito à proteção de dados, que são os mais diretamente afetados nestas situações. Via de regra, o empregador não poderá realizar averiguações sobre o estado de saúde do trabalhador, a não ser que seja relevante para constatar a aptidão para o trabalho. Em outros termos, somente poderão ser objeto de tratamento os dados estritamente necessários para o desempenho da atividade laboral, e não apenas convenientes ou úteis para a organização empresarial, pois a perspectiva será sempre de proteção do trabalhador[286].

Decisões empresariais aparelhadas em uma enfermidade estigmatizadora como a COVID que afetam trabalhadores saudáveis (*v.g.* despedida diante da recusa em se vacinar – sem valorar-se neste momento se o empregador está legitimado a conhecer essa informação) devem ser consideradas nulas, na medida em que o mero risco potencial de contágio não justifica a adoção de medidas preventivas desta natureza e podem conduzir à discriminação[287].

Em suma, os direitos de privacidade, de proteção de dados e de não discriminação coíbem a tomada de decisões empresariais baseadas em mera probabilidade estatística de que a pessoa possa vir a sofrer uma enfermidade ou uma limitação de suas condições físicas, impedindo, assim, a indagação sobre o estado de saúde do trabalhador quando não houver qualquer vinculação com a prevenção de riscos laborais. Ter-se-ia, portanto, como

---

284 Iván Antonio Rodríguez Cardo – *Prohibición de discriminación en el trabajo por razón de covid*. Pamplona: Aranzadi–Thomson Reuters, 2021, p. 48-56.

285 *Ibid.*, p. 57-64.

286 *Ibid.*, p. 57-64.

287 *Ibid.*, p. 114-115.

ilegítima a investigação sobre a imunidade de trabalhador saudável, máxime quando a decisão resultar prejudicial a este trabalhador (*v.g.* decisão de não contratação ou de extinção do contrato por elevada predisposição a padecer de determinada enfermidade)[288].

A busca por maior benefício empresarial, fora do âmbito da prevenção de riscos laborais, não é justificativa para desvendar informações de particular sensibilidade do empregado, como aquelas relativas à sua saúde. O direito à proteção de dados atua como limite específico dos poderes empresariais, de modo que quanto maior for o risco para os direitos e liberdades dos titulares dos dados, caso dos dados sensíveis, maior será a necessidade de estabelecerem-se salvaguardas adequadas.

A OIT já demonstrou preocupação em relação a não discriminação no tratamento de dados quando, no Repertório de recomendações práticas sobre proteção dos dados pessoais dos trabalhadores, aprovado em 1997, deixou assente que a utilização dos dados pessoais não deve comportar, direta ou indiretamente, uma discriminação contra indivíduos ou grupos de trabalhadores[289]. Especificamente sobre o assunto, o Comité Europeu de Proteção de Dados ressaltou que a extensão da utilização do Certificado Verde Digital - o fato de ter sido (ou não) vacinado ou recuperado do COVID-19 - para outros âmbitos, como o laboral, não deve conduzir legal ou factualmente à discriminação[290].

Sob o risco de incorrer-se em conduta discriminatória, a investigação sobre o estado de saúde do trabalhador deve se limitar a constatar a aptidão psicofísica do trabalhador para o desempenho da atividade laboral. Assim, a menos que haja alguma conexão com a prevenção dos riscos laborais, entendemos que o empregador não pode obter informação ou tomar uma decisão prejudicial ou pejorativa com base em dados de índole meramente probabilística[291].

No mesmo sentido vai a disposição do art. 25, n. 2, CT, que estabelece não configurar discriminação o comportamento baseado em factor de discriminação que constitua um requisito justificável e determinante para o exercício da actividade profissional, em virtude da natureza da actividade em causa ou do contexto da sua execução, devendo o objectivo ser legítimo e o requisito proporcional. *A contrario sensu* e indo ao encontro do que aqui

---

288 Iván Antonio Rodríguez Cardo – *Prohibición de discriminación en el trabajo por razón de covid*. Pamplona: Aranzadi–Thomson Reuters, 2021, p. 64-69.

289 Disponível em: https://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf (15.4.2022).

290 EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate), 31 March 2021. Disponível em: https://edps.europa.eu/system/files/2021-04/21-03-31_edpb_edps_joint_opinion_digital_green_certificate_en_0.pdf (15.4.2022).

291 Iván Antonio Rodríguez Cardo – *Prohibición de discriminación en el trabajo por razón de covid*. Pamplona: Aranzadi–Thomson Reuters, 2021, p. 122-123.

defendemos será discriminatória a prova da imunização quando esta não constituir em requisito justificável e determinante para o exercício da actividade profissional ou, noutras palavras, quando não houver conexão com a prevenção dos riscos laborais.

16. PROTEÇÃO DE DADOS E *STATUS* DA VACINAÇÃO

A pandemia do coronavírus, para além de reflexos na saúde pública, tem abalado o direito à privacidade dos indivíduos. O processamento de informações pessoais tem se mostrado bastante útil na execução de políticas para o enfrentamento da pandemia, mas deve-se questionar até que ponto tal utilidade é realmente benéfica: O interesse coletivo legitima toda e qualquer limitação ao direito à privacidade ou há limites ao tratamento e divulgação desses dados em situações como a atual? O combate ao COVID-19 justifica danos colaterais ao indivíduo decorrentes do tratamento de seus dados pessoais?[292]

A importância da privacidade e da proteção de dados foi destacada por várias legislações em todo o mundo, sendo o objetivo comum de todas elas promover a proteção das informações pessoais processadas por órgãos públicos e privados, dentre as quais se inclui o *status* da vacinação dos indivíduos no contexto do combate à pandemia do COVID-19[293].

A confirmação da vacinação contra o COVID-19 passou a ser exigida como condição para viajar, entrar em espaços públicos e até para aceder ao local de trabalho, sendo que a exigência para este último caso tem provocado intensos debates e resultado em diferentes abordagens ao redor do mundo[294].

---

[292] Jessica Andrade Modesto; Marcos Erhadt Júnior – Danos colaterais em tempos de pandemia: preocupaçãoes quanto ao uso dos dados pssoais no combate à covid-19. In Rodrigo Nóbrega FARIAS; Igor De Lucena MASCARENHAS (orgs.) – *COVID-19: saúde, judicialização e pandemia*. Curitiba: Juruá Editora Juruá, 2020, p. 149-152.

[293] Disponível em: https://www.rsm.global/insights/gdpr/covid-19-vaccination-status-and-data-privacy (19.7.2022).

[294] "The approaches taken to the collection and processing of vaccination data across the EU and the UK are varied. Several countries including Belgium, France, Germany, Italy, the Netherlands, and Ireland have issued guidance indicating that employers are not permitted to ask employees about their vaccination status because there is no valid legal basis to do so. In some countries, such as the Netherlands and Italy, if employees disclose information relating to their vaccination status to occupational health physicians, the physician may be permitted to process health data in certain circumstances (*e.g.,* the Netherlands permits processing of such data in the event of absenteeism or reintegration of employees), but will be bound by confidentiality obligations and therefore cannot disclose this information to the employer. That said, inquiries of a general nature may be allowed (*e.g.,* the Italian regulations permit an employer to ask the occupational health physician whether an employer is fit for work). By contrast, other countries such as Austria, Finland, Spain and the United Kingdom permit an employer to collect health data from employees

Os empregadores enfrentam o dilema de exigir que seus funcionários sejam vacinados ou comprovem seu estado de vacinação[295]. São frequentes as dúvidas sobre se realmente podem ou não perguntar aos empregados acerca do seu *status* de vacinação e, em caso afirmativo, como é que poderão proceder ao processamento de tais informações[296].

Como analisado no tópico anterior, medidas adotadas pelas empresas no âmbito da prevenção de riscos laborais, para garantir a segurança do local de trabalho, devem ser consideradas justas, especialmente quando não existirem alternativas menos intrusivas para alcançar-se o mesmo resultado. Com efeito, em contextos específicos de emprego, as vacinas podem ser consideradas uma medida de segurança necessária para funcionários que trabalham em hospitais, instalações médicas, serviços de emergência ou qualquer outro serviço de saúde da linha de frente[297].

Assim, em determinadas situações específicas e com vistas a cumprir a obrigação geral de garantir um local de trabalho seguro e minimizar o risco de exposição ao COVID-19, estarão os empregadores legitimados a perguntar sobre o *status* de vacinação de seus funcionários[298]. Em todo o caso, a informação deverá ser recolhida para fins específicos e legítimos e na medida do estritamente necessário para proteger os direitos à vida e à saúde, pois o tratamento desse tipo de informação também pode vulnerar algumas liberdades individuais, como a privacidade dos indivíduos, além de pôr em causa um dado sensível relativo à saúde dos indivíduos, que, como tal, somente pode ser objeto de tratamento em circunstâncias muito limitadas e está sujeito a normas de proteção mais rigorosas[299].

Desse modo, mesmo quando a coleta e o processamento da situação vacinal dos funcionários de uma empresa for expressamente autorizada pelo Poder Público, o empregador deverá ser extremamente cauteloso e seguir

---

to the extent that the information is necessary to ensure the safety of the workplace (*i.e.,* to prevent infections at the workplace). This processing of data is based on Article 9(2)(b) of the GDPR, which permits the processing of health data "for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment." Disponível em: https://www.insideprivacy.com/covid-19/covid-19-processing-of-vaccination-data-by-employers/ (11.4.2022).

295 Disponível em: https://www.dataguidance.com/opinion/europe-covid-19-vaccination-status-what-can (11.4.2022).

296 Disponível em: https://www.insideprivacy.com/covid-19/covid-19-processing-of--vaccination-data-by-employers/ (11.4.2022).

297 Disponível em: https://www.insideprivacy.com/covid-19/covid-19-processing-of--vaccination-data-by-employers/ (11.4.2022).

298 Diponível em: https://www.insideprivacy.com/covid-19/covid-19-processing-of--vaccination-data-by-employers/ (30.3.2022).

299 Disponível em: https://www.insideprivacy.com/covid-19/covid-19-processing-of--vaccination-data-by-employers/ (30.3.2022).

rigorosamente os termos da legislação de proteção de dados[300], dada a especial sensibilidade que é revestida esse tipo de informação. Como advertem Jessica Andrade Modesto e Marcos Erhadt Júnior, a tutela do direito à saúde, privacidade e proteção de dados devem coexistir[301].

Abaixo serão expostas considerações acerca dos requisitos necessários para coletar, processar e divulgar as informações pessoais relacionadas ao *status* de vacinação e sobre as medidas organizacionais e técnicas razoáveis que podem ser adotadas pelo empregador/responsável pelo tratamento a fim de salvaguardar os direitos e liberdades do titular dos dados/empregado.

16.1. A COLETA E O PROCESSAMENTO DE DADOS SOBRE A SITUAÇÃO VACINAL À LUZ DO RGPD

Para além da discussão acerca da obrigatoriedade da vacinação, surge um novo questionamento em face do RGPD[302]: Pode o empregador exigir de seus empregados a apresentação do comprovante de vacinação, que revela uma informação sensível?

Cumpre ressaltar que a condição de vacinado ou não do empregado, enquanto dado relativo à saúde, é um dado pessoal que revela uma informação sensível do trabalhador, e, como tal, possui uma proteção reforçada no RGPD, ante o seu potencial discriminatório elevado. Portanto, além de cumprir os requisitos gerais de proteção de dados, é preciso atentar-se às regras especiais que regem os dados sensíveis.

Antes de mais nada, é preciso ter em mente que o RGPD se aplica ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento manual ou por meios não automatizados de dados pessoais contidos em ficheiros[303] ou a eles destinados (art. 2, n. 1, RGPD). Isto significa dizer que caso a empresa realize apenas uma verificação visual do certificado de vacinação, porém não retenha nenhum dado pessoal, então não será o caso de aplicar-se o regime previsto no RGPD. Ao reverso,

---

300 Disponível em: https://www.rsm.global/insights/gdpr/covid-19-vaccination-status-and-data-privacy (30.3.2022).

301 Jessica Andrade Modesto; Marcos Erhadt Júnior – Danos colaterais em tempos de pandemia: preocupaçãoes quanto ao uso dos dados pssoais no combate à covid-19. In Rodrigo Nóbrega FARIAS; Igor De Lucena MASCARENHAS (orgs.) – *COVID-19: saúde, judicialização e pandemia*. Curitiba: Juruá Editora Juruá, 2020, p. 150.

302 "From a privacy perspective vaccine mandates are effectively a single exchange of data. An employee, for example, delivers proof of vaccination once and the employer makes a record of that event. Privacy protections apply to that single data record". David SELLA-VILLA – The COVID-19 Pandemic One Year On: Finding Balance Between Privacy and Public Health. *The Business Lawyer*. Vol. 77 (Ago 2021). DOI: http://dx.doi.org/10.2139/ssrn.3917827.

303 Segundo o Art. 4º/6 do RGPD, ficheiro corresponde a qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico.

se houver alguma espécie de processamento do dado, o empregador deverá atentar-se à disciplina específica do regime jurídico da proteção de dados.

Como esclarece Iván Antonio Rodríguez Cardo, o direito à proteção de dados não protege qualquer informação que o empregador venha a conhecer, ele é um direito instrumental que pretende garantir que o armazenamento da informação pessoal é seguro e que seu uso se vincula ao fim correto. O direito à proteção de dados não deriva automaticamente da afetação ao direito à privacidade, ou seja, de que certa informação seja ou não conhecida, mas que seja objeto de efetivo tratamento[304].

Em sendo a informação recolhida objeto de efetivo tratamento ou destinada a ser incluída em um ficheiro suscetível de tratamento, a primeira providência a ser tomada pelos empregadores é buscar uma base legal apropriada para processá-la.

Como já referido, o art. 9 do RGPD proíbe o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa, salvo se o tratamento puder ser reconduzido a uma das exceções elencadas no seu número 2, dentre as quais nos releva mencionar as seguintes alíneas: *a)* se o titular dos dados der o seu consentimento explícito; *b)* se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social; *g)* se o tratamento for necessário por motivos de interesse público importante; *h)* se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social; *i)* se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos.

Sem embargo, para que o tratamento de dados relacionados à saúde seja legítimo, não é suficiente o enquadramento numa das bases jurídicas ordinariamente previstas no art. 6º do RGPD, mas, mais que isso, é preciso superar-se a proibição de tratamento do dado pertencente à referida categoria

[304] Iván Antonio Rodríguez Cardo – *Prohibición de discriminación en el trabajo por razón de covid*. Pamplona: Aranzadi–Thomson Reuters, 2021. p. 84.

especial, que se dará quando as circunstâncias elencadas no n.º 2 do art. 9º do RGPD for observada[305].

Pois bem. A exceção prevista na alínea *b)* reflete o reconhecimento, por parte do legislador europeu, do dever de proteção do empregador para com seus trabalhadores frente os riscos laborais, devendo aquele garantir a segurança e a saúde de todos os trabalhadores a seu serviço em todos os aspectos relacionados com o trabalho[306]. Neste caso, para que o empregador possa proceder ao tratamento de dados de seus funcionários, é primordial a observância do requisito da necessidade, que pressupõe cumulativamente: *i)* a existência de suporte legal bastante – pode se fundar tanto em fontes imediatas do Direito como em convenções coletivas de trabalho; e *ii)* a existência de uma relação direta entre o tratamento e o cumprimento das obrigações ou o exercício do direito[307].

As exceções elencadas nas alíneas *g)* e *i)* podem ser examinadas conjuntamente, tendo em conta que ambas fazem referência a um interesse público, sendo que enquanto a primeira faz referência a um interesse qualificado como importante, a segundo faz referência a um interesse público qualificado no âmbito da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde, ambos com base no direito da União ou de um Estado-Membro que preveja medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados[308]. Apesar do paralelo que se possa fazer entre a alínea *g)* do art. 9, n. 2, RGPD, e da alínea *e)* do art. 6, n. 1, RGPD, na medida em que ambos se fundam no interesse público, o primeiro dispositivo faz referência ao adjetivo importante, o que reflete a natureza sensível dessa categoria de dados e o risco associado ao seu tratamento para o titular dos dados[309].

A exceção disposta na alínea *h)* permite o tratamento para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social. A diferença substancial entre essa exceção e a da alínea *i)* é

---

305 José Luis Domínguez Álvarez. La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19. *Revista de Comunicación y Salud*. Vol. 10, nº 2 (2020), p. 607-624. Disponível em: http://www.revistadecomunicacionysalud.es/index.php/rcys/article/view/240/197 (25.3.2022).

306 Agencia Española de Protección de Datos. Informe Jurídico 0017/2020. Madrid, 2020. Disponível em: https://www.aepd.es/es/documento/2020-0017.pdf (25.3.2022).

307 António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 137.

308 Agencia Española de Protección de Datos. Informe Jurídico 0017/2020. Madrid, 2020. Disponível em: https://www.aepd.es/es/documento/2020-0017.pdf (25.3.2022).

309 António Barreto Menezes Cordeiro – *Direito da Proteção de Dados à luz do RGPD e da Lei nº 58/2019*. Coimbra: Almedina, 2020. p. 248.

que a primeira visa, preferencialmente, a proteção de interesses individuais, enquanto a segunda tem por escopo a proteção de interesses coletivos[310].

O consentimento do empregado - exceção prevista na alínea *a)* -, como já aprofundado em tópico apartado, raramente é apropriado no contrato de trabalho, em virtude da típica assimetria entre as partes jurídicas existente nesse tipo relação.

Todavia, como se vê, mesmo que excluído o consentimento, a coleta de dados sensíveis pode amparar-se em qualquer outra base legal. É possível, inclusive, que mais de uma base legal justifique um mesmo tratamento de dados. Por exemplo, a recolha do dado vacinal de empregado pode ser necessária tanto para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, como para efeitos de medicina preventiva ou do trabalho e prestação de cuidados ou tratamentos de saúde ou prestação de cuidados ou tratamentos de saúde ou por motivos de interesse público no domínio da saúde pública (hipóteses previstas nas alíneas *b)*, *h)* e *i)* do número 2 do artigo 9, RGPD).

É imperioso destacar que, mesmo num contexto de emergência em saúde pública, o regime jurídico de proteção de dados previsto no RGPD há de ser respeitado, uma vez que a crise, por si só, não legitima ingerências excessivas na esfera jurídica da liberdade individual (e, de igual forma, na privacidade). Quaisquer restrições ou ingerências requerem preocupações éticas no tocante à privacidade e à proteção de dados pessoais[311].

Segundo o Comité Europeu de Proteção de Dados "mesmo nestes tempos excecionais, a proteção dos dados pessoais tem de ser mantida em todas as medidas de emergência, incluindo nas restrições adotadas no plano nacional em conformidade com o artigo 23, contribuindo para o respeito pelo valores estruturantes da democracia, do Estado de Direito e dos direitos fundamentais em que se funda a União; por um lado, qualquer medida adotada pelo Estado-Membro tem de respeitar os princípios gerais de direito, o conteúdo essencial dos direitos fundamentais e liberdades, e não pode ser irreversível, e, por outro lado, os responsáveis pelos tratamentos e os subcontratantes têm de continuar a cumprir as regras de proteção de dados"[312].

---

310 António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 140-141.

311 Patrícia Cardoso Dias – Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública. *Julgar On-line*. Jan. 2021. Disponível em: http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/ (22.3.2022).

312 Statement on restrictions on data subject rights in connection to the state of emergency in Member States, de 2 de junho de 2020, § 4º. Disponível em: https://edpb.europa.

Tem-se, portanto, que, inclusive em circunstâncias excepcionais, deve-se assegurar o respeito pelos princípios básicos concernentes à proteção de dados, particularmente os princípios da proporcionalidade e da minimização de dados[313], principalmente quando o tratamento envolve dados especialmente sensíveis, como o são os dados relativos à saúde, que, como tal, possuem íntima e estreita ligação com os direitos e liberdades fundamentais[314].

Importa mencionar que o legislador europeu previu a possibilidade de limitação pelos Estados-Membros, por meio de medida legislativa, de um conjunto de normas, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar interesses públicos, entre os quais se destaca a saúde pública[315]. Porém, não se encontram entre o conjunto de normas que podem ser limitadas aquelas que tratam sobre as condições de licitude dos tratamentos de dados pessoais, mais especificamente os artigos 6 e 9 do RGPD, de maneira que os seus termos devem ser observados na íntegra[316].

Logo, considerando-se que a prova de imunização diz respeito ao tratamento de dados relativos à saúde, por conseguinte, dados sensíveis, deve-se observar, de antemão, as condições de licitude para o tratamento previstas no artigo 9 do RGPD, mesmo em momentos de crise sanitária como a que ora se vivencia.

Como analisado acima, há entendimentos, com bons fundamentos, que divergem acerca da permissibilidade acerca da requisição pelo empregador da prova de vacinação de seu empregado. No nosso entendimento, o tratamento só deve ocorrer quando restar provado, no caso em concreto, que o conhecimento do *status* da vacinação está fundamentado em motivos convincentes ou é realmente necessário para os efeitos previstos no RGPD para o tratamento dos dados sensíveis[317].

---

eu/our-work-tools/ourdocuments/other/statement-restrictions-data-subject-rights-connection-state_en (15.4.2022).

313 Statement on the processing of personal data in the context of the COVID-19 outbreak, de 19 de março de 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf (15.4.2022).

314 José Luis Domínguez Álvarez. La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19. *Revista de Comunicación y Salud*. Vol. 10, nº 2 (2020), p. 607-624. Disponível em: http://www.revistadecomunicacionysalud.es/index.php/rcys/article/view/240/197 (25.3.2022).

315 Vide art. 23 do RGPD.

316 Orientações sobre os tratamentos de dados pessoais de saúde regulados no Decreto nº 8/2020, de 8 de novembro. Disponível em: https://www.cnpd.pt/media/1bbppegs/orienta%C3%A7%C3%B5es_decreto_8_2020.pdf (10.3 2022).

317 Disponível em: https://portal.oa.pt/comunicacao/imprensa/2021/06/29/foi-barrado-na-sua-empresa-por-nao-estar-vacinado-lei-nao-permite-mas-ha-excecoes/ (10.3.2022).

Assim, antes que se proceda à coleta do *status* de vacinação dos trabalhadores, é fundamental analisar se a coleta é, de fato, justificada. O setor de atuação da organização, o tipo de trabalho que a equipe desempenha e os riscos para a saúde e segurança no local de trabalho são aspectos a serem levados em consideração quando da coleta de tal informação. Dentre outras situações, será considerada justificável a coleta nos locais que representam um risco para indivíduos clinicamente vulneráveis (*v.g.* ambiente de assistência social e de saúde).[318]

Para Iván Antonio Rodríguez Cardo a legitimidade da investigação empresarial varia de acordo com a concreta atividade que realiza o trabalhador e, em particular, se gera um risco específico de exposição a agentes biológicos determinados, como o coronavírus. As ações do empregador devem estar orientadas a eliminar o risco ou diminuir a probabilidade de que o trabalho cause danos ao trabalhador, ou seja, o propósito das normas de prevenção de riscos laborais consiste em evitar que o trabalhador se contagie no trabalho, e não a proteger em abstrato a saúde do trabalhador[319]. Estas considerações são importantes na avaliação do teste de proporcionalidade.

Embora se reconheça a utilidade da vacinação, o Comité da Convenção 108 adverte que nenhuma discriminação injustificada pode ocorrer com base no fato de uma pessoa não ter sido vacinada, seja qual for o motivo, e determina que seja assegurado o respeito estrito do direito à proteção de dados[320].

Adicionalmente, o direito europeu e o direito interno, designadamente o RGPD e a Lei n. 58/2019, que assegura a execução na ordem jurídica interna do RGPD em matéria de proteção de dados, não obstam a coleta de dados de saúde (no caso, o conhecimento do *status* da vacinação dos empregados), apenas impõem que os dados pessoais tratados sejam necessários para atingir as finalidades visadas, finalidades estas que devem ser lícitas e não discriminatórias. Adverte-se, ainda, que, caso a coleta de informações sobre a vacina possa gerar uma discriminação negativa (*v.g.* negação de uma oportunidade de emprego), os cuidados despendidos pelo empregador devem ser redobrados[321].

É preciso ressaltar que todas as exceções elencadas no n. 2 do art. 9, RGPD, pressupõem o elemento da necessidade, que deve ser preenchido por referência ao princípio da proporcionalidade, optando-se sempre pela

---

318 Disponível em: https://www.migalhas.com.br/depeso/348419/respostas-as-principais-duvidas-dados-de-colaboradores-vacinados (19.7.2022).

319 Iván Antonio Rodríguez Cardo – *Prohibición de discriminación en el trabajo por razón de covid*. Pamplona: Aranzadi–Thomson Reuters, 2021. p. 37.

320 Disponível em: https://www.coe.int/en/web/human-rights-rule-of-law/-/covid-19-vaccination-attestations-and-data-protection (19.7.2022).

321 Disponível em: https://www.insideprivacy.com/covid-19/covid-19-processing-of-vaccination-data-by-employers/ (30.3.2022).

solução menos intrusiva na esfera privada do titular[322] e com respeito ao princípio da minimização de dados, significando dizer que os dados tratados deverão de ser exclusivamente limitados aos necessários para a finalidade pretendida, sem que se possa confundir conveniência com necessidade[323]. Consoante Menezes Cordeiro, deve-se considerar como necessário todo o tratamento que caso não ocorra termine por implicar ou não impedir a produção de danos gravosos, respeitando-se o sempre presente princípio da minimização de dados[324].

Ainda segundo Menezes Cordeiro, o princípio da minimização de dados é composto por três pilares: *(i)* adequação; *(ii)* pertinência; *(iii)* limitação. De acordo com o citado autor, a adequação impõe aos responsáveis pelo tratamento que circunscrevam a recolha e demais tratamentos a dados pessoais que se insiram nas finalidades perseguidas; a pertinência circunscreve as atividades dos responsáveis a tratamentos que possam contribuir para a prossecução dessas finalidades; e, por fim, destaca que o tratamento será juridicamente aceitável apenas se não houver um método alternativo menos intrusivo dos direitos dos titulares[325]. No mesmo sentido estipula o artigo 29 da Lei n. 58/2019, de 8 de agosto[326] que "Nos tratamentos de dados de saúde e de dados genéticos, o acesso a dados pessoais rege-se pelo princípio da necessidade de conhecer a informação".

Mafalda Miranda Barbosa salienta que, para se concluir justificadamente pela legitimação do tratamento, será fundamental que ele se afigure necessário, não podendo esta necessidade – atento aos valores em causa – equivaler à mera aptidão das medidas para lidar com o surto epidémico, é preciso que haja um controlo legitimador que seja imposto pelo critério da necessidade, ou seja, o tratamento de dados deve obedecer uma ideia de proporcionalidade. Isto significa dizer que algumas das medidas adotadas para fazer frente ao surto epidémico podem ficar comprometidas se não se revelarem imprescindíveis (e não meramente aptas)[327]. Assim, antes de tudo, deve-se questionar se a recolha dos dados, no caso a prova de vacinação dos empregados, é realmente necessária/imperiosa ou se o mesmo objetivo pode ser atingido de outra maneira.

---

322 António Barreto Menezes Cordeiro – *Direito da Proteção de Dados à luz do RGPD e da Lei nº 58/2019*. Coimbra: Almedina, 2020. p. 247.

323 Agencia Española de Protección de Datos. Informe Jurídico 0017/2020. Madrid, 2020. Disponível em: https://www.aepd.es/es/documento/2020-0017.pdf (25.3.2022).

324 António Barreto Menezes Cordeiro – *Op. cit.,* p. 243.

325 António Barreto Menezes Cordeiro (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021. p. 105.

326 Legislação que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

327 Mafalda Miranda Barbosa – *Direito (Civil) em tempos de pandemia*. 1ª ed. Coimbra: Gestlegal, 2021. p. 85.

Com base no princípio da concordância prática, a ingerência no domínio da saúde individual, valor eminentemente pessoal, precisa ser justificada perante os benefícios coletivos que podem ser atingidos a partir da recolha desse tipo de dado considerado sensível. Haverá de ponderar-se, no caso em concreto, se os meios utilizados são efetivos e proporcionados aos objetivos de saúde pública[328]. Nesta senda, com vistas a atenuar o impacto negativo na privacidade, a investigação acerca da condição de vacinado ou não de um empregado apenas será considerada legítima quando for estritamente necessária ou quando não houver outros meios menos invasivos para se alcançar as finalidades almejadas.

De todo modo, em que pese os diferentes posicionamentos que gravitam em torno do debate, o fato é que, em determinadas situações, o empregador poderá, preenchido o pressuposto da necessidade, requisitar de seus empregados o comprovante de vacinação com fundamento numa das bases legais supraelencadas.

Independentemente da imposição da obrigação de vacinação no local de trabalho, pode ser que o empregador necessite conhecer a condição da vacinação do funcionário para saber o procedimento que deve adotar caso o empregado futuramente venha a ser exposto ao vírus, uma vez que este poderá variar dependendo se o empregado é vacinado ou não. Por exemplo, enquanto um funcionário totalmente vacinado que era exposto ao COVID-19 e estava assintomático não precisava ficar em quarentena ou ser impedido de trabalhar, um funcionário não vacinado precisava ficar de quarentena, mesmo que não apresentasse sintomas, para evitar a propagação do vírus[329].

Porém, em todo e qualquer caso, deverá observar-se o princípio da minimização dos dados, devendo os dados ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados, não se podendo estender o dito tratamento a quaisquer outros dados pessoais não estritamente necessários para a finalidade prosseguida, tampouco a pessoas que não tenham necessidade de os conhecer. Na prática, os empregadores que optarem por coletar as informações de vacinação devem ter o cuidado de restringir o acesso a tais informações, sempre que possível, aos setores de saúde ocupacional ou recursos humanos[330], não

---

328 Patrícia Cardoso Dias – Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública. *Julgar On-line*. Jan. 2021. Disponível em: http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/ (22.3.2022).

329 H. R. Falks. Covid-19 employer liability still unknown. *Court Review*, Vol. 57, nº 3 (2021), p. 164-171.

330 Disponível em: https://br.lexlatin.com/opiniao/lgpd-e-os-cuidados-na-coleta-de-dados-de-vacinacao-de-funcionarios (22.3.2022).

sendo por isso mesmo permitido o compartilhamento entre os colegas de trabalho[331]. A confidencialidade é reforçada pelo dever de sigilo a que estão obrigados todos aqueles que tenham acesso a dados relativos à saúde, nos termos do n. 4 do art. 29 da LE.

A exclusiva aplicação da normativa de proteção de dados pessoais permite que o responsável pelo tratamento adote decisões que sejam necessárias para o cumprimento de obrigações legais ou para a salvaguarda de interesses essenciais no âmbito da saúde pública, devendo em todo o caso respeitar o conteúdo essencial do direito à proteção de dados e as medidas adequadas e específicas para proteger os interesses e direitos fundamentais do interessado[332].

A Comissão Nacional de Proteção de Dados (CNPD), nas orientações sobre recolha de dados de saúde dos trabalhadores, adverte que as entidades empregadoras devem se abster de adotar iniciativas que impliquem a recolha de dados pessoais de saúde dos seus trabalhadores, por serem dados sensíveis reveladores de aspetos da vida privada destes, quando as mesmas não tenham base legal, nem tenham sido ordenadas pelas autoridades administrativas competentes. Na sequência, todavia, salienta que a eventual recolha de informação relativa à saúde ou à vida privada do mesmo relacionada com a sua saúde (*v.g.*, se esteve em contacto com pessoas contaminadas) apenas está legitimada se for realizada direta e exclusivamente pelo profissional de medicina no trabalho, que deverá adotar os procedimentos adequados a salvaguardar a saúde dos próprios e de terceiros[333].

Com efeito, por serem os dados pessoais relacionados à saúde considerados dados sensíveis, reveladores de aspectos da vida privada do trabalhador e com potencial de gerar ou aumentar a discriminação, o Direito vigente prevê a adoção de medidas específicas adicionais visando salvaguardar os direitos e liberdades do titular dos dados e reduzir os riscos provenientes desse tratamento, em particular o sigilo profissional[334].

Mesmo nos casos em que o tratamento seja possível, as informações deverão ser prestadas ao médico, cabendo a este apenas comunicar ao empregador se o empregado está ou não apto para desempenhar a actividade.

---

331 Lauren Chalaturnyk – Covid-19 vaccines in the workplace: employees. *LawNow*. Vol. 45, nº 5 (2021), p. 36-38.

332 José Luis Domínguez Álvarez. La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19. *Revista de Comunicación y Salud*. Vol. 10, nº 2 (2020), p. 607-624. Disponível em: http://www.revistadecomunicacionysalud.es/index.php/rcys/article/view/240/197 (25.3.2022).

333 Disponível em: https://www.cnpd.pt/media/bq5byjzb/orientacoes_recolha_dados_saude_trabalhadores.pdf (15.2.2022).

334 Orientações sobre recolha de dados de saúde dos trabalhadores. Disponível em: https://www.cnpd.pt/media/bq5byjzb/orientacoes_recolha_dados_saude_trabalhadores.pdf (19.7.2022).

Ou seja, o empregador deverá ser comunicado apenas se o empregado foi ou não vacinado. Não lhe interessa saber quando, onde e qual foi a vacina que o empregado recebeu[335].

Ainda que a investigação sobre a condição de vacinado não seja considerada um exame médico, é preciso cautela por parte dos empregadores, uma vez que que perguntas relativas à condição de vacinado do empregado constitui, em última instância, uma investigação relacionada ao seu estado de saúde[336], que pode resultar em discriminação no ambiente de trabalho e até mesmo fora dele.

Por envolverem informações médicas confidenciais, o empregador deverá adotar todos os cuidados necessários quanto ao seu armazenamento, incluindo a destinação das informações coletadas, seja a terceiros ou até a funcionários internos, uma vez que eventual violação pode provocar uma séria ameaça à privacidade[337]. Deverá, assim, adotar as medidas oportunas de seguridade e responsabilidade proativa que o tratamento requer (art. 32, RGPD)[338] e assegurar um padrão de segurança e qualidade em relação ao tratamento dos dados pessoais necessários, visando cumprir o critério superior de *privacy by design* e *privacy by default* (art. 25, RGPD)[339], de modo que a privacidade e a proteção de dados se integrem a todo o ciclo de vida da tecnologia, desde a primeira fase da concepção até seu uso e sua eliminação[340]. A adoção de medidas de segurança adequadas está em consonância com o princípio da integridade e da confidencialidade, o qual estabelece que os dados sejam tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito[341], o que supõe, logicamente, a reserva sobre a identidade dos trabalhadores

---

335 Lauren Chalaturnyk – Covid-19 vaccines in the workplace: employees. *LawNow*. Vol. 45, nº 5 (2021), p. 36-38.

336 Margaret R. Kurlinski – COVID-19: An Employer's Role in Vaccination. *Corporate Counsel.* Vol. 35, nº 1 (2021), p. 4-7. Ver também: What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws. Disponível em: https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws (19.7.2022).

337 Lauren Chalaturnyk – *Op. cit.*, p. 36-38.

338 Agencia Española de Protección de Datos. Informe Jurídico 0017/2020, Madrid. Disponível em: https://www.aepd.es/es/documento/2020-0017.pdf (25.3.2022).

339 Patrícia Cardoso Dias – Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública. *Julgar On-line*. Jan. 2021. Disponível em: http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/ (22.3.2022).

340 Juan Francisco Rodríguez Ayuso – *Privacidad y Coronavirus*: aspectos esenciales. Madrid: Dykinson, S.L., 2021. p. 167.

341 Disponível em: https://br.lexlatin.com/opiniao/lgpd-e-os-cuidados-na-coleta-de-dados-de-vacinacao-de-funcionarios (22.3.2022).

contagiados ou até mesmo não vacinados para evitar o estigma social que eventualmente desemboca na discriminação[342].

Também será preciso certificar-se de que os empregados entendam os motivos por que a empresa precisa coletar os seus dados. A transparência é fundamental para a redução dos riscos envolvendo o monitoramento da vacinação dos funcionários[343].

Além disso, os empregadores devem registrar com precisão as informações que coletam e garantir que a coleta e o armazenamento sejam seguros[344]. Precisam, também, ter atenção ao prazo de retenção e meios de descarte dos dados coletados[345], devendo mantê-los apenas durante o período necessário para as finalidades para as quais são tratados.

Uma vez coletados dados dessa natureza, eles devem ser mantidos em segurança, ficar sujeitos aos deveres de confidencialidade existentes e ser retidos pelo prazo mínimo necessário para cumprir sua finalidade legítima, respeitada sempre a transparência para com os funcionários em relação aos motivos para a recolha de tais informações e como elas serão usadas[346].

O respeito aos princípios gerais relativos ao tratamento de dados pessoais consagrados no n. 1 do artigo 5, conjuntamente com a adoção de todas as medidas específicas e adequadas com vista à defesa dos direitos fundamentais e dos dados pessoais dos titulares - e a necessária comprovação da eficácia das medidas adotadas conforme resulta do princípio de *accountability* previsto no n. 2 do mesmo artigo[347] – impõem também a realização de uma avaliação de impacto[348] para formalização da análise de riscos e a adoção de outras medidas para mitigar os riscos, se a utilização dos dados for capaz de gerar um risco elevado para a privacidade dos indivíduos[349]. Quanto mais elevado for o risco para os direitos e liberdades das pessoas

---

342 Iván Antonio Rodríguez Cardo – *Prohibición de discriminación en el trabajo por razón de covid*. Pamplona: Aranzadi–Thomson Reuters, 2021. p. 81.

343 Disponível em: https://br.lexlatin.com/opiniao/lgpd-e-os-cuidados-na-coleta-de-dados-de-vacinacao-de-funcionarios (22.3.2022).

344 Disponível em: https://www.migalhas.com.br/depeso/348419/respostas-as-principais-duvidas-dados-de-colaboradores-vacinados (22.3.2022).

345 Idem.

346 Disponível em: https://www.insideprivacy.com/covid-19/covid-19-processing-of-vaccination-data-by-employers/ (30.3.2022).

347 Disponível em: http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/ (22.3.2022).

348 Nos termos da acepção do art. 35, nº 3, b), a realização de uma avaliação de impacto sobre a proteção de dados é obrigatória nas operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9º, nº 1, dentre os quais estão incluídos os dados relativos à saúde.

349 Disponível em: https://www.migalhas.com.br/depeso/348419/respostas-as-principais-duvidas-dados-de-colaboradores-vacinados (30.3.2022).

singulares, maior será a cautela exigida no tratamento. Nesta senda, considerando evidente o alto risco para os direitos e liberdades fundamentais, Juan Francisco Rodríguez Ayuso adverte para a necessidade de que todo tratamento de dados relativos à saúde, implementado com o objetivo de proteger as pessoas no contexto da pandemia do coronavírus, seja precedido de uma análise de riscos que, antecipando-se aos problemas, proponha respostas e determine o conjunto de medidas de seguridades aplicáveis[350].

Por veicularem informação de grande sensibilidade, os dados relativos à saúde estão submetidos a regras de proteção reforçadas tendentes a assegurar um nível de segurança adequado ao risco de violação de direitos fundamentais que lhes é inerente. Os empregadores devem adotar todas as medidas condizentes às melhores práticas de privacidade ou as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo a pseudonimização[351], a realização de auditorias e a manutenção de um arquivo com informações relativas à vacinação separado dos arquivos pessoais dos funcionários[352]. Essas e outras medidas, como aquelas que o legislador europeu apresenta no art. 32, n. 1, RGPD, podem ser implementadas, consoante a situação concreta, com vistas a reduzir os riscos envolvidos. E, como forma de comprovar a adoção dessas medidas técnicas e organizativas adequadas, o empregador/responsável pelo tratamento pode invocar o cumprimento de um código de conduta ou de um procedimento de certificação aprovados, respectivamente, nos moldes dos artigos 40 e 42[353].

À luz de todas essas considerações, tem-se que após o enquadramento em uma das exceções à regra proibitiva do tratamento, listadas no art. 9, n. 2, RGPD, toda e qualquer operação de tratamento de dado relativo à saúde, no caso a coleta sobre informação relativa ao *status* de vacinação do empregado, deverá respeitar rigorosamente os princípios da minimização dos dados, da exatidão, da limitação do período de conservação e da integridade e confidencialidade, devendo o tratamento ser sempre efetuado por profissionais de saúde habilitados para o efeito e observar todas as medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.

---

350 Juan Francisco Rodríguez Ayuso – *Privacidad y Coronavirus*: aspectos esenciales. Madrid: Dykinson, S.L., 2021. p. 167-187.

351 "la pseudonimización [...] no es sino una (si bien de las más importantes) de las medidas de seguridad, técnicas y organizativas, que podrá adoptar el responsable para hacer frente al riesgo que conlleve el tratamiento". *Ibid.*, p. 151. Ver também a definição do art. 4º/5, RGPD.

352 David Sella-Villa – The COVID-19 Pandemic One Year On: Finding Balance Between Privacy and Public Health. *The Business Lawyer*. Vol. 77 (Ago 2021). DOI: http://dx.doi.org/10.2139/ssrn.3917827.

353 Vide Art. 24º/3, RGPD.

17. CONCLUSÃO

A crise sanitária provocada pela pandemia do novo coronavírus impôs que as autoridades públicas e privadas implementassem medidas tendentes a prevenir e mitigar o contágio, colocando-se ainda mais em evidência as discussões em torno da privacidade e da proteção de dados, dentre as quais mereceu a atenção deste trabalho a investigação realizada pelos empregadores sobre o *status* da vacinação dos seus funcionários.

O debate tem polarizado as opiniões em torno da legitimidade sobre esse tipo de investigação, *maxime* porque o regime jurídico vigente não exclui em absoluto a possibilidade de as empresas solicitarem dos empregados informações relativas ao assunto ou exigirem a prova da imunização, mas principalmente porque não existe, pelo menos em Portugal, uma legislação que preveja expressamente a obrigatoriedade da vacinação contra a COVID-19.

Para além disso, tal investigação envolve informações sensíveis, por veicularem dados pessoais relativos à saúde, que podem ser reveladoras de aspectos da vida privada com potencial discriminatório e atentatório a outros direitos fundamentais, podendo ser ainda mais problemática na relação de emprego, que, como se sabe, é marcada pela típica assimetria das posições jurídicas do empregado e empregador[354].

Desta sorte, em virtude da particular sensibilidade que o tratamento desses dados envolve, principalmente dentro do contexto laboral, resulta do próprio princípio da proibição do excesso ou da proporcionalidade em sentido amplo (art. 18, n. 2, CRP) que a informação relativa à condição de vacinação do empregado apenas seja objeto de tratamento quando for estritamente necessária para as finalidades a que se propõe ou quando constituir um requisito justificável e determinante para o exercício da actividade profissional, em virtude da natureza da função em causa ou do contexto da sua execução (art. 25, n. 2, CT). A título exemplificativo, consideramos legítima a coleta de informações dessa natureza naquelas atividades que lidam, por exemplo, com indivíduos clinicamente vulneráveis, como os hospitais e os lares de idosos.

Isso significa que as empresas devem nortear-se por normas de prevenção de riscos laborais, e não propriamente por normas de saúde pública. Ou seja, elas não estão legitimadas a promover incursões na esfera privada dos trabalhadores por mera conveniência ou sob a abstrata justificativa de salvaguardar a saúde e segurança do local de trabalho. É preciso, na verdade, que haja um risco acrescido de propagação do vírus no ambiente de traba-

---

354 Conforme exposto no Acórdão n.º 368/2002 do Tribunal Constitucional, não há como negar que a prova de imunização traduz-se, em certos casos, um ónus para a obtenção do emprego e, noutros casos, um verdadeiro dever jurídico para a própria manutenção da relação laboral.

lho, que variará dependendo da atividade explorada e das condições em que esta atividade é exercida.

Outrossim, devido à proximidade com a esfera mais pessoal e/ou íntima do titular e do risco de discriminação que está associado ao processamento dos dados relativos à saúde, o seu tratamento demanda uma proteção qualificada e superior relativamente ao tratamento dos demais dados pessoais. As empresas devem proceder com cuidado redobrado ao decidirem ir a fundo nesse tipo de investigação, pois, em última análise, estar-se-á também restringindo o direito fundamental à reserva da vida privada da pessoa-trabalhadora, constitucionalmente consagrado no art. 26 e legislativamente no art. 26, CT, de modo que devem optar, se possível, pela solução menos intrusiva na esfera privada do titular.

À luz de todas essas considerações, uma vez autorizada incursão dessa natureza, é preciso que o tratamento desses dados proceda na estrita conformidade com os princípios de proteção de dados, nomeadamente o princípio da minimização dos dados, e que as empresas mantenham uma política de responsabilidade reforçada, o que deverá incluir a elaboração de um regulamento interno que disponha de maneira expressa e minuciosa sobre a possibilidade de exame de aspectos relacionados à imunização contra a COVID-19.

18. BIBLIOGRAFIA

Abbate-Dattilo, Pamela – Navigating the legal challenges of covid-19 vaccine policies in private employment: school vaccination laws provide roadmap. *Mitchell Hamline Law Review*. Vol. 47, nº 3 (2021), p. 1019.

Acórdão nº 288/1998 do Tribunal Constitucional.

Adragão, Paulo Pulido; Leão, Anabela Costa – O Direito à Objecção de Consciência por parte do Chefe de Estado, em Questão. O caso da recusa de promulgação de actos legislativos por motivo de consciência. In *AA. VV* – Estudos em Homenagem ao Professor Doutor Jorge Miranda. Coimbra: Coimbra Editora. Vol. 3 (2012).

Álvarez, José Luis Domínguez. La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19. *Revista de Comunicación y Salud*. Vol. 10, nº 2 (2020), p. 607-624. Disponível em: http://www.revistadecomunicacionysalud.es/index.php/rcys/article/view/240/197 (25.3.2022).

Amado, João Leal – Vacinação obrigatória para quem trabalha? *Observatório Almedina*. 12 Jan. 2022. Disponível em: https://observatorio.almedina.net/index.php/2022/01/12/vacinacao-obrigatoria-para-quem-trabalha/ (7.3.2022).

Andrade, João Carlos Vieira De – *Os Direitos fundamentais na Constituição Portuguesa de 1976*. 5ª ed. Coimbra: Almedina, 2016.

Antunes, Aquilino Paulo – Vacinas para a Covid-19: aspectos para reflexão. *Revista da Faculdade de Direito da Universidade de Lisboa*. Vol. 61, nº 2 (2020).

Areheart, Bradley A., Roberts, Jessica L – Gina, Big Data, and the Future of Employee Privacy. *The Yale Law Journal*. Vol. 128, nº 3 (2019), p. 710-791. Disponível em: https://www.yalelawjournal.org/pdf/AreheartRoberts_a2gvpzai.pdf (19.7.2022).

Barbosa, Mafalda Miranda – *Direito (Civil) em tempos de pandemia*. 1ª ed. Coimbra: Gestlegal, 2021.

Bioni, Bruno Ricardo – *Proteção de dados pessoais*: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2019.

Brown, Jessica; Elliot, Lauren J.; Rauch, Daniel – An employer playbook for the covid "vaccine wars": strategies and considerations for workplace vaccination policies. *Practical Lawyer*. Vol. 67, nº 1 (2021), p. 20-30.

Canas, Vitalino – *O princípio da proibição do excesso na conformação e no controlo de atos legislativos*. Coimbra: Almedina, 2017.

Canotilho, J.J. Gomes; Moreira, Vital – *Constituição da República Portuguesa Anotada*. Vol. I. 4ª ed. Coimbra: Coimbra Editora, 2007.

Cardo, Iván Antonio Rodríguez – *Prohibición de discriminación en el trabajo por razón de covid*. Pamplona: Aranzadi–Thomson Reuters, 2021.

Chalaturnyk, Lauren – Covid-19 vaccines in the workplace: employees. *LawNow*. Vol. 45, nº 5 (2021), p. 36-38.

Chemerinsky, Erwin; Goodwin, Michele – *Compulsory Vaccination Laws Are Constitutional*. Legal Studies Research Paper Series nº 2015-71. Vol. 110, nº 3 (2015).

Coelho, Diogo; Vitorino, José Miguel – Dos Direitos Fundamentais da vida privada do trabalhador e da sua tendencial limitação nas organizações de tendência. *Questões Laborais*. Coimbra: Almedina. Nº 49 (2017), 28p.

Cordeiro, António Barreto Menezes (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021.

Cordeiro, António Barreto Menezes. *Direito da Proteção de Dados à luz do RGPD e da Lei nº 58/2019*. Coimbra: Almedina, 2020.

Cordeiro, António Barreto Menezes – *O consentimento do titular dos dados no RGPD*. Lisboa: Universidade de Lisboa, 2018. Disponível em: https://blook.pt/publications/publication/e772e2d8f7b4/ (19.7.2022).

Correia, Victor – *Sobre a privacidade*. Óbidos: Sinapis, 2016.

Costa, Andréa Dourado; Gomes, Ana Virginia Moreira. Discriminação nas relações de trabalho em virtude da coleta de dados sensíveis. *Scientia Iuris*. Londrina. Vol. 21, nº 2 (Jul. 2017), p. 214-236.

Crespí Ferriol, Maria Del Mar – El tratamiento de los datos personales relativos a la salud de los trabajadores. *Revista General de Derecho del Trabajo y de la Seguridad Social*. Nº 52 (2019), p. 257-298. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=6876300 (18.7.2022).

Davidov, Guy – 7º Encontro Ibérico Transformações Recentes. Disponível em: https://www.youtube.com/watch?v=0Y8b0o7TLPA&t=8288s (9.5.2022).

Davidov, Guy – Non-waivability in Labour Law. *Oxford Journal of Legal Studies*. Vol. 40, nº 3 (2020), p. 10-18.

Dias, Patrícia Cardoso – Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública. *Julgar On-line*. Jan. 2021(tradução da autora). Disponível em: http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/ (22.3.2022).

Declaração Do Centenário Da Oit Para O Futuro Do Trabalho: adotada pela Conferência Internacional do Trabalho na sua 108ª sessão. União Geral de Trabalhadores (coord.). Lisboa. UGT, 2019. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-lisbon/documents/publication/wcms_749807.pdf (6.7.2021).

Duarte, Diogo Pereira – In CORDEIRO, António Barreto Menezes (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*. Coimbra: Almedina, 2021.

Escarpiado, Rita Isabel Ramos Batista – *Discriminação do trabalhador em razão do conhecimento da informação médica*: em especial os dados genéticos. Lisboa: Universidade de Lisboa, 2018. Dissertação para a obtenção do grau de Mestre em Direito e Prática Jurídica, especialidade Direito da Empresa. Disponível em: https://repositorio.ul.pt/bitstream/10451/37504/1/ulfd137176_tese.pdf (30.11.2021).

Estorninho, Maria João; Macieirinha, Tiago – *Direito da saúde* – Lisboa: Universidade Católica, 2014.

Falks, H. R. – Covid-19 employer liability still unknown. *Court Review*. Vol. 57, nº 3, p. 164-171.

Ferreira, António Casimiro – Sociedade da Austeridade e direito do trabalho de exceção. Coimbra: Vida Económica, 2012.

Godinho, João Carlos Carvalho – *A (re)discussão dos fundamentos da vacinação humana obrigatória*. Coimbra: Almedina, 2022.

Gomes, Carla Amado – *Defesa da Saúde vs. Liberdade Individual*: casos da vida de um médico de saúde pública. Lisboa: Associação Acadêmica da Faculdade de Direito de Lisboa, 1999.

Gouveia, Jorge Bacelar – Objecção de consciência (direito fundamental à). In Fernandes, José Pedro; Queiró, Afonso Rodrigues (coords.) – *Dicionário Jurídico da Administração Pública. Lisboa*. Vol. 6 (1994), p. 165 e ss.

Guimarães, Maria Raquel; Redinha, Maria Regina – A Portuguese approach to privacy in Covid-19 times: through the keyhole. In HONDIUS, Ewoud [et al.]. *Coronavirus and the law in Europe*. Intersentia, 2021. p. 1009-1026.

Guimarães, Rui [Et Al.] – Acesso e reutilização de registos clínicos para fins de investigação no âmbito da pandemia por COVID-19. *Revista do Ministério Público*. Vol. 163 (Jul./Set., 2020), p. 203-226.

Hernáiz, Elisa Sierra. *Las categorías especiales de datos del trabajador*: Estudio de los límites y garantías legales para su tratamiento en la relación laboral. Pamplona: Aranzadi–Thomson Reuters, 2021.

Irrazábal, Gabriela; Belli, Laura; Funes, María Eugenia – Direito à saúde *versus* objeção de consciência na Argentina. *Revista Bioética*. Brasília. Vol. 27, nº 4 (Out./Dez. 2019), p. 728-738. Disponível em: https://www.scielo.br/j/bioet/a/QsxNzMGKgRwsNpTz5KPmccQ/?lang=pt&format=pdf (18.5.2022).

Kurlinski, Margaret R. – COVID-19: An Employer's Role in Vaccination. *Corporate Counsel*. Vol. 35, nº 1 (2021), p. 4-7.

Lopes, Inês Maria Oliveira Gomes Camarinha – *O RGPD e a proteção dos dados sensíveis dos menores*. Porto: 17 Dez. 2020. Dissertação de mestrado apresentada à Faculdade de Direito da Universidade do Porto.

Lopes, Sónia Kietzmann – Direitos fundamentais e direitos de personalidade do trabalhador à luz do Código do Trabalho. In Direitos Fundamentais e de Personalidade do Trabalhador (3ª ed.). *Centro de Estudos Judiciários*. Jun. 2019, p. 25-36. Disponível em: http://www.cej.mj.pt/cej/recursos/ebooks/trabalho/eb_DireitoPersonalidade2019.pdf?id=9&username=guest (8.7.2022).

Marx, Karl – *O Capital*: Vol: 1. Editora Nova Cultural, [(1867:197)1996].

Mayer-Schönberger, Viktor; Cukier, Kenneth – *Big Data*: A Revolution that Will Transform how We Live, Work, and Think. Boston, New York, 2013.

Medeiros, Rui – Anotação ao artigo 64º. In Miranda, Jorge; Medeiros, Rui – *Constituição Portuguesa Anotada*. Vol. I, 2ª ed. revista. Coimbra: Coimbra Editora, 2010. p. 620.

Miranda, Jorge – *Direitos Fundamentais*. 3ª ed. Coimbra: Almedina, 2020.

Modesto, Jessica Andrade; Erhadt Júnior, Marcos – Danos colaterais em tempos de pandemia: preocupaçãoes quanto ao uso dos dados pssoais no combate à covid-19. In FARIAS, Rodrigo Nóbrega; MASCARENHAS, Igor de Lucena (orgs.) – *COVID-19: saúde, judicialização e pandemia*. Curitiba: Juruá Editora, 2020.

Moreira, Teresa Coelho – Algumas implicações laborais do Regulamento Geral de Proteção de Dados Pessoais no Trabalho 4.0. *Questões Laborais*. Coimbra: Almedina. Ano 24, nº 51 (2017), p. 9-34.

Moreira, Teresa Coelho – Algumas questões sobre trabalho 4.0. *4ª Revolução Industrial*. Ano IX, nº 86, Mar. 2020. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/170751/2020_moreira_teresa_questoes_trabalho.pdf?sequence=1 (6.7.2021).

Moreira, Tereza Coelho – As novas tecnologias de informação e comunicação e o poder de controlo eletrónico do empregador. In *Estudos do Direito do Trabalho*. Coimbra: Almedina, 2011. p. 11-34.

Moreira, Teresa Coelho – Dados pessoais: breve análise do art. 28º da Lei nº 58/2019, de 8 de agosto. *Questões Laborais*. Coimbra: Almedina. Ano XXVI, nº 55 (jul./dez. 2019), p. 41-62.

Moreira, Tereza Coelho – Da esfera Privada do Trabalhador e Controlo do Empregador. *Studia Iuridica 78*. Boletim da Faculdade de Direito da Universidade de Coimbra: Coimbra Editora, 2004.

Moreira, Tereza Coelho – "Novas Tecnologias: Um Admirável Mundo Novo do Trabalho?". In *Estudos do Direito do Trabalho*. Coimbra: Almedina, 2011.

Murcia, Joaquín García; Cardo, Iván Antonio Rodríguez – Implicaciones laborales del Reglamento 2016/679 de la Unión Europea sobre Protección de datos personales. *Questões Laborais*. Coimbra: Almedina. Ano 24, nº 51 (jul./dez. 2017), p. 35-67.

Novais, Jorge Reis – *Os princípios constitucionais estruturantes da República Portuguesa*. Coimbra: Coimbra Editora, 2004.

Organização Mundial Sobre O Futuro Do Trabalho – Trabalhar para um Futuro Melhor: Comissão Mundial sobre o Futuro do Trabalho. Lisboa: OIT, 2019.

Pinheiro, Alexandre Sousa (coord.) [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina, 2018.

Pinheiro, Alexandre Sousa – *Privacy e Protecção de Dados Pessoais*: A Construção Dogmática do Direito à Identidade Informacional. Lisboa: AAFDL, 2015.

Pinto, Paulo Mota – In *Direitos de Personalidade e Direitos Fundamentais*: Estudos. 2ª ed. Coimbra: Gestlegal, 2018.

Pinto Junior, Vitor Laerte – Anti-vacinação, um movimento com várias faces e consequências. *Cadernos Ibero-Americanos de Direito Sanitário*. Brasília. Vol. 8, nº 2 (2019), p. 116-122.

Ray, Jean-Emmanuel – Qualité de vie et travail de demain, *Droit Social*. Dialnet. Lisboa. ISSN 0012-6438. Nº 2 (2015), p. 147-154.

Ray, Jean-Emmanuel; Rojot, Jacques – Worker Privacy in France. *Comparative Labor aw Journal*. Vol. 17, nº 1 (1995), p. 61-74.

Redinha, Maria Regina Gomes – Da Protecção da Personalidade no Código do Trabalho. *Para Jorge Leite*: escritos jurídico-laborais. Coimbra: Coimbra Editora, 2014. p. 819-852.

Reis, Beatriz De Felipe – *O direito fundamental à proteção de dados pessoais e sensíveis do trabalhador frente às novas tecnologias da informação e comunicação*. Criciúma, 2019. Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade do Extremo Sul Catarinense (UNESC).

Reis, Raquel Tavares – *Liberdade de Consciência e de Religião e Contrato de Trabalho do Trabalhador de Tendência*: que equilíbrio do ponto de vista das relações individuais do trabalho? Coimbra: Coimbra Editora, 2004.

Riva, Michele Augusto; Paladino, Maria Emilia; Paleari, Andrea; Belingheri, Michael – Workplace COVID-19 vaccination, challenges and opportunities. *Occupational Medicine*. England: Oxford. Vol. 72, nº 4 (Maio 2022), p. 235-237.

Rodríguez Ayuso, Juan Francisco – *Privacidad y Coronavirus*: aspectos esenciales. Madrid: Dykinson, S.L., 2021.

Sarmento E Castro, Catarina – 40 anos de "utilização da informática": o artigo 35º da Constituição da República Portuguesa. *e-Pública*. Vol. 3, nº 3 (dez. 2016), p. 42-66. Disponível em: https://www.e-publica.pt/volumes/v3n3a04.html (19.7.2022).

Seira, César Cierco – La vacuna-condición o el pasaporte de vacunación y su eventual encaje en un marco general de vacunación recomendada contra la COVID-19. *National Library of Medicine*. Vol. 22, nº 2 (Maio/Ago 2021), p. 82-88.

Sella-Villa, David – The COVID-19 Pandemic One Year On: Finding Balance Between Privacy and Public Health. *The Business Lawyer*. Vol. 77 (Ago 2021).

Silva, Diogo Filipe Rodrigues Da – *Regulamento Geral de Proteção de Dados*: O Consentimento do Trabalhador. Porto: Out. 2020. Dissertação conducente à obtenção do Grau de Mestre em Direito pela Faculdade de Direito da Universidade do Porto.

Viapiana, Vitória Nassar; Gomes, Rogério Miranda; Albuquerque, Guilherme Souza Cavalcanti De – Adoecimento psíquico na sociedade contemporânea: notas conceituais a teoria da determinação social do processo saúde-doença. Saúde e Debate. Rio de Janeiro. Vol. 42, Nº Especial (Dez. 2018), p. 175-186. Disponível em: https://www.scielo.br/j/sdeb/a/Y36fDqvZL5Js4nnWpXrYpBb/?lang=pt# (10.2.2022).

Villalón, Jesús Cruz – El impacto de la digitalización sobre los derechos fundamentales laborales. In Royo, Miguel Rodríguez-Piñero; Todolí Signes, Adrián (coords.) – *Vigilância y control en el Derecho del Trabajo Digital*. Pamplona: Aranzadi–Thomson Reuters, 2020.

III

OS CONTRATOS SOBRE DADOS

O QUADRO NORMATIVO E JURISPRUDENCIAL PARA OS FLUXOS TRANSATLÂNTICOS DE DADOS PESSOAIS

Patrícia Pereira Paredes

pasederap@hotmail.com

Resumo: Com o título "O Quadro Normativo e Jurisprudencial para os Fluxos Transatlânticos de Dados Pessoais", a presente dissertação propõe-se a escrutinar as sucessivas alterações concernentes ao quadro regulatório das transferências transatlânticas (UE-EUA) de dados pessoais. Tal análise irá ser feita tendo em consideração não só o quadro jurídico-normativo europeu aplicável ao longo das últimas décadas, mas também a jurisprudência do Tribunal de Justiça da União Europeia, considerando as consecutivas invalidações de decisões de adequação adotadas pela Comissão Europeia relativamente aos Estados Unidos da América, nomeadamente (i) a decisão de adequação "Porto Seguro" (Decisão 2000/520/CE da Comissão, de 20 de julho de 2000), e (ii) a decisão de adequação "Escudo da Privacidade" (Decisão 2016/1250/CE da Comissão, de 12 de julho de 2016).

Palavras-Chave: União Europeia; Proteção de Dados Pessoais; Transferências Transatlânticas de Dados; RGPD; Decisão "Porto Seguro"; Decisão "Escudo Da Privacidade"; Estados Unidos da América.

Abstract: Entitled "The Normative and Jurisprudential Framework for Transatlantic Flows of Personal Data", this dissertation aims to scrutinize the successive changes concerning the regulatory framework for transatlantic (EU-US) transfers of personal data. Such analysis will be carried out taking into account not only the European legal-normative framework applicable over the last few decades, but also the jurisprudence of the Court of Justice of the European Union, considering the consecutive invalidations of adequacy decisions adopted by the European Commission in relation to the United States of America, namely (i) the "Safe Harbour" adequacy decision (European Commission Decision 2000/520/EC, 20th of July of 2000), and (ii) the "Privacy Shield" adequacy decision (European Commission Decision 2016 /1250/EC, 12th of July of 2016).

Keywords: European Union; Protection of Personal Data; Transatlantic Data Transfers; GDPR; "Safe Harbor" Decision; "Privacy Shield" Decision; USA.

1. INTRODUÇÃO

Os desenvolvimentos tecnológicos das últimas décadas e o eclodir de novos meios de informação e de comunicação, aliados a uma assumida intensificação e proliferação do processo da globalização, vieram revolucionar a forma através da qual se procede ao tratamento de dados pessoais nas suas diversas etapas (a saber, a colheita, o armazenamento e a partilha).

Os fenómenos referidos (i.e., os desenvolvimentos tecnológicos e a intensificação dos processos de globalização), permitem-nos, desde já e na linha de Menezes Cordeiro, proceder a uma delimitação teleológica da ratio deste ramo do Direito:

> *"(…) tanto numa perspetiva histórica, como numa perspetiva dogmática atual, a produção legislativa relativa aos dados pessoais justificou- se não para acautelar os interesses individuais dos titulares dos dados – esses seriam sempre protegidos através da invocação de normas gerais relativas aos direitos de personalidade – mas para regular o seu tratamento."*[1]

Ora, por outras palavras, a ideia da "proteção de dados pessoais" remete-nos para o fornecimento de instrumentos legais de proteção e salvaguarda

[1] António Menezes Cordeiro, "*Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019*", Editora Almedina, 2020

contra o uso inapropriado da tecnologia de processamento de informação – em constante mutação e evolução -, e não, verdadeiramente, para o embargo ou oposição ao processamento de tais informações.

Na decorrência do exposto supra, e volvido um período tendencialmente associado a um mais conservador e moroso tratamento dos dados pessoais, a nova Era Digital fez-se acompanhar de um colossal crescimento do tratamento automatizado de dados – manifestamente mais célere e massivo –, que veio possibilitar a realização de um manuseamento dos dados a uma velocidade e numa quantidade sem precedente até à época. Tal circunstância veio determinar que as transferências de dados pessoais viessem a adquirir um papel primordial no âmbito da atual economia de informação.

A título de exemplo, o relatório da *IBM Marketing Cloud* de 2016, reconhecida plataforma internacional de marketing digital, veio constatar que 90% dos dados no mundo, à data de 2016, haviam sido criados apenas nos dois anos antecedentes, asseverando, assim, o peso notório que estes representam no plano da contemporânea economia digital global.

Dessarte, o peso e o impacto associado a esta economia digital colocaram-na no plano de atuação europeu, convertendo-a num autêntico interesse público primário a ser prosseguido pela União Europeia, nomeadamente mediante a introdução de um Mercado Único Digital.

Porém, e não obstante o impacto – económico, mas não só – que a mera posse de dados pessoais hodiernamente representa, o cidadão comum continua sem compreender, na sua plenitude, a razão pela qual os seus dados pessoais são de tal forma desejáveis pelas mais diversas entidades, sejam elas de natureza pública ou privada. Nesta medida, poder-se-ia questionar o que poderá conter de tão relevante estes dados pessoais informatizados, a ponto de o Tribunal de Justiça da União Europeia (doravante, TJUE), desde o acórdão *Lindqvist* –mas também de *Scarlet*, *Digital Rights*, *Google*, *Schrems*, *Tele 2*, etc. – ter travado uma autêntica guerra com o intuito de que o legislador europeu lograsse em adotar o atual Regulamento Geral de Proteção de Dados (doravante, RGPD).

Com base no exposto supra, e não descurando a complexidade intrínseca a esta temática, a relevância atribuída à colheita, armazenamento e tratamento de dados pessoais é, na realidade, deveras simples: em suma, a livre circulação de dados é indispensável para o desenvolvimento da chamada economia digital, não havendo nenhum ator na cena internacional que, partindo de uma lógica comercial, pretenda ficar excluído desta autêntica oportunidade de comércio e protagonismo político, aumentando, desta forma, a sua presença, influência e poderio na negociação e no contexto europeu e internacional.

Por conseguinte, os dados pessoais assumem hoje uma posição de verdadeiros ativos que, enquanto tal, são suscetíveis de serem comercializados em todo o globo, pelos mais diversos atores – atores estes cuja legitimidade e *modus operandi* de colheita, armazenamento e tratamento é, não raramente, ética e/ou juridicamente questionável.

À face do exposto supra, dever-se-á considerar que a regulamentação das transferências de dados pessoais assume, hoje, uma posição de capital relevância para todas as pessoas, de natureza singular ou coletiva, sob pena da ocorrência de eventuais violações suscetíveis de lesar os interesses e os direitos, absolutos e/ou relativos, dos titulares destes dados – situação que, pela importância e pessoalidade que estes dados materializam, deverá ser categoricamente evitada.

Outrossim, a expressão de que os dados pessoais são o "petróleo do século XXI"[2], cunhada a propósito das potencialidades da *Big Data*, demonstra uma convicção clara da sua indiscutível importância no panorama jurídico e económico, numa perspetiva local, regional e global. Uma nítida manifestação desta potencialidade foi demonstrada, inclusive, pelo Parlamento Europeu através de um Briefing publicado a 8 de janeiro de 2020 das empresas com maior poderio económico relativamente aos anos de 2008 e 2018. De acordo com este *briefing* comparativo, se em 2008 os lugares cimeiros da tabela eram ocupados por empresas petrolíferas e energéticas (entre as quais *PetroChina, Exxon*, etc.), em 2018 esses mesmos lugares foram ocupados por empresas tecnológicas (entre as quais *Apple, Google, Microsoft, Amazon e Facebook*).

Todavia, a emergência desta *data economy* coloca-nos, indubitavelmente, numa posição de fragilidade e de manifesta incerteza tendo em consideração que, apesar de o Direito da proteção de dados pessoais não se tratar de um ramo jurídico novo (*v.g.,* na União Europeia, no Estado de *Hesse*, na Alemanha, a primeira lei relativa à proteção de dados pessoais foi aprovada em 1970[3]), ele apenas recentemente assumiu uma importância inegável e, consequentemente, somente ultimamente têm surgido reais desafios à garantia da tutela dos dados pessoais, impondo aos diversos Estados, organizações internacionais e indivíduos, a necessidade da adoção de uma postura ativa e, simultaneamente, preventiva.

Uma clara manifestação deste último corolário pode ser exemplificada através da pesquisa promovida pela Conferência das Nações Unidas para o Comércio e Desenvolvimento, que veio constatar que 137, de um total de 194, países implementaram legislações com o intuito de regular as políticas de dados pessoais. Deste modo, podemos atualmente afirmar que cerca de 71% dos países do mundo promulgaram normas sobre proteção de dados pessoais, o que demonstra de forma clara e evidente a importância que os Estados atribuem à regulação dos fluxos de informações na Era Digital e os perigos decorrentes da falta dessa regulamentação.

---

[2] Meglena Kuneva, Roundtable on Online Data Collection, Targeting and Profiling, Bruxelas, 31 de março de 2009, em "*Personal data is the new oil of the internet and the new currency of the digital world*.".

[3] Para mais detalhes sobre a evolução histórica do Direito alemão da proteção de dados veja-se: J. Collin Bennett, "*Regulating Privacy: Data Protection and Public Policy in the Europe and the United States*", Cornell University Press, 1992.

Desta forma, poder-se-á incontestavelmente concluir que os dados pessoais são expressão direta da dignidade humana[4], elemento indissociável da vida privada dos seus titulares, e direito fundamental garantido pela Carta dos Direitos Fundamentais da União Europeia (CDFUE). Tais particularidades determinam que eles merecem uma garantia de proteção adequada – conceção que o TJUE veio afirmar com a jurisprudência que irá ser objeto de análise mais adiante.

Deste modo, a União Europeia, enquanto organização internacional supranacional, dotada de personalidade jurídica e agindo no âmbito das suas competências, em conformidade com o princípio da atribuição (previsto no artigo 4º do Tratado sobre o Funcionamento da União Europeia, doravante TFUE), e na decorrência do fenómeno da "europeização" de certas matérias, viu-se na necessidade de atuar neste domínio com vista a garantir uma maior centralidade ao direito fundamental à proteção dos dados pessoais, permitindo o florescimento e desenvolvimento da economia digital. Assim, podemos concluir que este regime consagra "duas das mais antigas e igualmente importantes ambições do processo de integração europeia": a proteção dos direitos fundamentais e a realização do mercado interno, em especial a livre circulação de dados pessoais[5].

A introdução de instrumentos jurídicos que harmonizassem o direito interno dos Estados-Membros nesta temática consubstanciou uma parte considerável da atuação das instituições e órgãos europeus. A título de exemplo, observámos a introdução de um pacote de reformas em matéria de proteção de dados, adotado pela União Europeia em 2016, no qual se inclui o vigente Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE). A introdução desta fonte de direito derivado, dotada de efeito direto, nos termos do artigo 288º do TFUE, veio assumir dois grandes propósitos: "(i) defender os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção de dados, 1º/2; e (ii) promover a livre circulação dos dados pessoais, 1º/3."[6].

Mas a atuação das instituições europeias não se esgota nesta tendencial homogeneização dos regimes jurídicos aplicáveis nos diversos Estados-Membros. Deste modo, a União Europeia tem vindo, simultaneamente, a avançar com a celebração de acordos comerciais de cooperação com países terceiros, a fim de estabelecer uma base legal comum que permita o

---

4 Filipa Urbano Calvão, "*A protecção de dados pessoais na internet: desenvolvimentos Recentes*", Revista de Direito Intelectual, 2015/2.

5 Comissão Europeia, "*Uma abordagem global da proteção de dados pessoais na União Europeia*", de 4 de novembro de 2010.

6 António Menezes Cordeiro, "*Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019*", Editora Almedina, 2020.

intercâmbio de informações, fortalecendo, assim, as trocas comerciais e a cooperação internacional.

As Decisões da Comissão 2000/520/CE de 20 de julho de 2000 e 2016/1250/CE de 12 de julho de 2016 relativamente a um dos seus maiores e mais antigos parceiros comerciais, os EUA, funcionaram como fundamento para acordos desse tipo. Note-se que as relações com os EUA, sejam elas de natureza política, económica ou de segurança, são de capital relevância para a União Europeia, encontrando-se alicerçadas numa multiplicidade de fatores, como veio constatar a Comissão Europeia já em 1995, numa comunicação sua ao Parlamento, reforçando os pontos em comum entre estes dois atores internacionais.

Ora, se é verdade que entre o período que medeia 1995 e a atualidade a matéria da proteção de dados pessoais sofreu uma inequívoca evolução, também não poderemos negligenciar o facto de que esta evolução veio impactar as relações entre Estados, mas também entre estes e os seus cidadãos, estendendo-se a todo o território europeu, mas também a um panorama internacional, designadamente nos fluxos transatlânticos, criando climas de confiança, mas por vezes gerando climas de suspeição, e até algum ceticismo, relativamente à verdadeira eficácia e proteção garantida pelo Direito Europeu intra e além fronteiras.

Mas há também que salientar que o debate sobre o âmbito de aplicação extraterritorial do regime de proteção de dados pessoais da União Europeia não se trata de uma polémica recente e, "após um período em que passou amplamente despercebido, a discussão foi instigada pela decisão *Google Spain*. Neste caso, o Tribunal de Justiça da União Europeia (TJUE) concluiu que a Diretiva 95/46/CE se aplicava às atividades da *Google Inc*., uma empresa estabelecida nos EUA."[7], afirmando, desta forma, que a legislação europeia aplicar-se-ia, indiretamente, a países terceiros.

Ora, ainda que na linha de alguns autores pudéssemos questionar acerca da legalidade desta decisão por parte do TJUE, não poderemos nunca descorar que em causa estão direitos fundamentais – e estes valem na sua plenitude num Estado de Direito Democrático, devendo ser sempre plenamente protegidos e garantidos, independentemente do território e do sistema jurídico em apreço.

Assim, cumpre atentar mais detalhadamente à evolução do regime jurídico-normativo europeu para as transferências de dados pessoais.

---

[7] Graça Canto Moniz, "*Breves reflexões sobre o enquadramento normativo do Regulamento Geral de Proteção de Dados Pessoais (RGPD)*", Centro de Estudos Judiciários, Outubro de 2021.

2. EVOLUÇÃO HISTÓRICA DO REGIME JURÍDICO-NORMATIVO EUROPEU PARA A PROTEÇÃO DE DADOS PESSOAIS

"Foi preciso o colapso total da Europa e o declínio económico e político do Velho Continente para se lançar as bases da renovação e para que a ideia de uma nova ordem europeia ganhasse uma renovada dinâmica."[8]. Foi com base nesta lógica assente numa conjuntura política e social indiscutivelmente degradada e empobrecida, que nasceu um dos maiores e mais ambiciosos projetos políticos da História da Humanidade: a contemporânea União Europeia, uma união económica e política de – presentemente – 27 Estados-membros.

A afirmação da União Europeia como uma União de Direito implica que esta não possa ignorar as novas exigências que se vão sentido, nomeadamente aquelas impostas pelo surgimento progressivo de um – cada vez mais - *homo digitalis*. "A montante, o sentido cada vez mais (assumidamente) político do aprofundamento da integração, bem como a prioridade colocada na construção da cidadania europeia e no reforço de uma dimensão de integração extraeconómica, tudo isso favorece o desenvolvimento de uma cultura de direitos fundamentais europeia."[9] – direitos fundamentais estes que não podem ser alienados e alheados àquilo que corresponde à realidade digital contemporânea.

Porém, se *ab initio* a construção de um regime jurídico-normativo europeu para a proteção de dados pessoais se apresentou como um fenómeno moroso e de difícil homogeneização, considerando a – ainda atual – intransigência por parte dos Estados na cessão da sua soberania em determinados domínios, nomeadamente nos da privacidade e da proteção de dados, na última década as instituições europeias vieram colocá-lo no âmago do atual processo de aprofundamento europeu, introduzindo pacotes de reformas legislativas, elaborando doutrina e proferindo jurisprudência – em suma, concertando atuações e propugnando valores que, seguramente, se têm vindo a revelar indispensáveis para a concretização de uma verdadeira economia digital, de um Mercado Único Digital e de um crescente integracionismo europeu assente na proteção dos direitos dos cidadãos europeus.

E se este integracionismo em matéria de proteção de dados já se encontrava em curso, o impulso sentido pela adoção do RGPD, em 2016, foi, sem sombra para dúvidas, um passo considerável no sentido de uma plena homogeneização do direito aplicável à proteção dos dados pessoais e, inquestionavelmente, um triunfo dos compromissos assumidos pelos princípios europeus.

---

8 Klaus-Dieter Borchardt, "*O ABC do direito da União Europeia*", 2016.

9 Alessandra Silveira & Pedro Froufe, "*Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos*", UNIO EU Law Journal, Vol. 4, No. 2, Julho 2018

Deste modo, atente-se à evolução que o direito europeu da proteção de dados pessoais teve desde 1950 até aos dias de hoje.

2.1. NO DIREITO DO CONSELHO DA EUROPA

Se apenas em 1951, com a assinatura do Tratado de Paris que instituiu a Comunidade Europeia do Carvão e do Aço (CECA), os políticos europeus iniciaram o processo de construção daquilo que hoje conhecemos como União Europeia, já um ano antes, em 1950, o Conselho da Europa, almejando a defesa do direito à privacidade, dava um importante contributo na proteção dos dados pessoais[10] ao adotar a Convenção Europeia dos Direitos Humanos (CEDH).

Nos termos do artigo 8.º desta Convenção, o direito à proteção contra a recolha e utilização de dados pessoais integra o direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência. Esta Convenção, com tanto de revolucionária como de necessária considerando a complexidade dos desafios sociais, políticos e económicos que se faziam agourar à data, possibilitou que se assegurasse um novo sistema de garantias jurídicas relativas à proteção dos direitos humanos, permitindo aos órgãos instituídos em Estrasburgo punir quaisquer violações destes.

Todavia, com o surgimento da tecnologia da informação na década de 60, sentiu-se uma crescente necessidade de adotar regras mais pormenorizadas de salvaguarda dos dados pessoais, com vista a colmatar as lacunas oriundas dos desafios colocados pela introdução destas novas tecnologias e a densificar a proteção por estas colocada em causa.

Neste sentido, o Comité de Ministros do Conselho da Europa adotou, nos anos 70, variadas resoluções com vista a densificar e garantir a efetiva tutela dos dados pessoais. A título de exemplo, poder-se-ia aludir à Resolução 73/22, relativa à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de dados no setor privado, de 26 de setembro de 1973, e a Resolução 74/29, relativa à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de dados no setor público, de 20 de Setembro de 1974, do Comité de Ministros do Conselho da Europa.

---

[10] Heraclides Dos Santos Silva, "*A Protecção de Dados Pessoais na Era Global: O Caso Schrems*", Universidade Nova de Lisboa, 2017: "O direito à protecção de dados pessoais é reconhecido ao nível internacional em vários instrumentos adoptados sob a égide da Organização das Nações Unidos, sendo na maioria dos casos como uma extensão do direito à privacidade. Neste sentido, ver o art. 12.º da Declaração Universal dos Direitos Humanos; o art. 17.º do Pacto Internacional sobre os Direitos Civis e Políticos; o Comentário Geral n.º 16 sobre o direito ao respeito da privacidade, família, domicílio e correspondência, e protecção da honra e reputação – art. 17.º; e as Directrizes Para a Regulação de Ficheiros Informatizados de Dados de Carácter Pessoal, adoptadas pela Resolução 45/95 da Assembleia Geral das Nações Unidas, de 14 de Dezembro de 1990.".

Já em 1981, foi aberta para assinatura a Convenção do Conselho da Europa para a Proteção de Indivíduos Relativamente ao Tratamento Automático de Dados Pessoais, comumente designada por Convenção 108. Até hoje, a Convenção 108 foi o primeiro - e único - acordo multilateral juridicamente vinculativo no domínio da proteção de dados.

Há que salientar que, não obstante esta Convenção ter sido ratificada pela totalidade dos Estados-Membros da União Europeia, em 1999 a Convenção 108 foi sujeita a alterações com vista a permitir a adesão da própria União Europeia – adesão, porém, que nunca veio a ter lugar.

Em grande medida, mas não exclusivamente, os objetivos da implementação desta Convenção passavam, principalmente, por reforçar a proteção da privacidade no espaço digital, procurando proteger os particulares de qualquer abuso que pudesse ocorrer com a recolha e tratamento dos seus dados, nomeadamente através da consagração de diversas garantias jurídicas e, na falta destas, a proibição do tratamento de dados sensíveis, tais como os dados alusivos à raça, à opinião política, às convicções religiosas, à saúde, à vida sexual ou ao registo criminal.

Com base em alterações supervenientes, datadas de 2001, a Convenção propôs-se a regular o fluxo transfronteiriço de dados pessoais, adicionado um protocolo respeitante aos fluxos transfronteiriços de dados pessoais direcionado a transferências para Estados terceiros, isto é, Estados não signatários da Convenção, que previa uma nova obrigação de criação de autoridades nacionais de controlo de proteção de dados, ampliando, desta forma, a proteção destes.

Posteriormente, com o intuito de desenvolver os princípios gerais e regras estabelecidos na Convenção, o Comité de Ministros do Conselho da Europa adotou várias recomendações, *práxis* que ainda hoje mantém.

Todavia, a caminho dos quarenta anos de existência, esta Convenção encontrava-se parcialmente ultrapassada. Tal decorria, maioritariamente, do facto de ter sido aberta para assinatura muito antes da era da Internet e das comunicações eletrónicas, contexto que conduz a que se mostre "já datada em alguns dos conceitos e soluções propostos, facto exponenciado pela híper-evolução a que se assistiu nas últimas décadas em matéria de tratamentos de dados pessoais, seja na sua quantidade, seja na sofisticação e complexidade que cada vez mais apresentam"[11].

Neste sentido, em Junho de 2018, foi aprovado pela Comissão Europeia a Proposta de Decisão do Conselho que autorizava os Estados-Membros a ratificar o Protocolo de Alteração que viria reformar a Convenção n.º 108. As alterações introduzidas por este Protocolo posicionam, hoje, a Convenção 108, agora designada de Convenção 108+, num patamar significativamente superior quanto ao nível de garantia de proteção dos dados pessoais compa-

[11] Cnpd, PARECER/2019/1, de 7 de janeiro de 2019, da Comissão Nacional de Proteção de Dados.

rativamente ao nível de proteção assegurado pela anterior Convenção, aproximando-se nitidamente à proteção garantida pelo quadro normativo do RGPD.

Aliás, no Parecer n.º 2019/1, de 7 de janeiro de 2019, a Comissão Nacional de Proteção de Dados, veio apontar as modificações mais relevantes à presente Convenção, a saber:

> A considerável diminuição de exceções à aplicação da Convenção;
>
> A evolução em termos concetuais (nomeadamente a mais aprofundada especificação do princípio do tratamento lícito, em particular no que concerne aos requisitos aplicáveis ao consentimento);
>
> O reforço à proteção de categorias especiais de dados (alargando simultaneamente as categorias àquelas que são reconhecidas como categorias especiais de dados pessoais no direito da União);
>
> A previsão de garantias suplementares para os particulares cujos dados pessoais sejam objeto de tratamento (em especial a obrigação de examinar o impacto provável de uma operação de tratamento de dados prevista e de adotar as medidas técnicas e organizacionais necessárias; e a obrigação de comunicar violações graves de dados);
>
> E o reforço dos direitos dos particulares, nomeadamente no que diz respeito à transparência e no acesso aos dados, assim como no surgimento do direito de se oporem ao tratamento dos seus dados.

2.2. NO DIREITO DA UNIÃO EUROPEIA

Não obstante os avanços feitos pelos Conselho da Europa, não podemos descurar a ideia de que "o Conselho da Europa 'foi menos bem sucedido em termos de assegurar consistência suficiente em todos os Estados-Membros', e uma maior ação legislativa tornou-se necessária"[12]. A criação de um regime jurídico tendencialmente mais uniforme e relativamente mais harmonizado, que se mostrasse eficaz na proteção dos dados pessoais e, simultaneamente, suscetível de ser irradiado dentro e fora do espaço europeu, tornou-se, além de desejável, progressivamente impreterível.

Um primeiro passo no sentido deste aprofundamento assinalou-se com a entrada em vigor da Diretiva 95/46/CE, de 24 de Outubro de 1995, comumente conhecida como Diretiva de Proteção de Dados (DPD).

A adoção deste instrumento de direito derivado ocorreu num período durante o qual na maioria dos Estados-Membros já vigoravam leis internas que regulavam a proteção de dados, pelo que um dos principais desígnios da aludida diretiva passou por harmonizar estas legislações internas, com vista a alcançar a existência, no território europeu, de um padrão mínimo de proteção dos direitos e liberdades dos cidadãos quando estivesse em causa o tratamento dos seus dados pessoais.

---

12 Peter Hustinx, "*EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*", 2014.

Segundo o Considerando n.º 11 da Diretiva, as suas finalidades primordiais consistiam em clarificar e ampliar os princípios da Convenção n.º 108, destacando a necessidade de garantir que a circulação transfronteiriça de dados pessoais fosse realizada de forma regulada, com vista a não impedir a livre circulação de dados pessoais entre Estados-Membros.

Assim, exagerado não será dizer que este instrumento formou a base do desenvolvimento das legislações nacionais de cada Estado-Membro no que respeita à matéria da proteção de dados à data de 1995.

No cumprimento dos trâmites desta Diretiva, "foi estabelecido um regime geral de proteção de dados no território europeu, sujeitando o tratamento de dados pessoais a critérios de necessidade, pertinência e não excessividade em função às finalidades prosseguidas e limitando, em termos genéricos, a sua conservação ao período necessário para a prossecução das finalidades para que os mesmos são recolhidos ou para que devem ser tratados posteriormente"[13], não havendo margem para a existência de tratamentos arbitrários e/ou desmesurados.

Naturalmente, a vigência de um regime dotado das características supra acarretaria, indiscutivelmente, inúmeros benefícios no âmbito da consolidação do projeto europeu e do seu desenvolvimento económico. Porém, o aprofundamento da regulamentação europeia por esta via de atuação não teve êxito, uma vez que o processo legislativo de transposição não foi realizado de forma homogénea pelos Estados-Membros, subsistindo uma fragmentação e discrepância no nível de proteção dos dados pessoais dentro do território europeu. Aliás, nesse mesmo sentido aponta a Comissão Europeia, à data da proposta do, agora vigente, RGPD:

> *«As diferenças entre os Estados-membros quanto ao nível de proteção dos direitos e das liberdades das pessoas, nomeadamente do direito à proteção dos dados pessoais, no que respeita ao tratamento desses dados, podem impedir a livre circulação de dados pessoais no conjunto da União. Estas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas ao nível da UE, falsear a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Estas diferenças nos níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE.»*[14].

Uma vez que a Diretiva não era aplicável ao tratamento de dados pessoais no âmbito da cooperação policial e judiciária em matéria penal, o Conselho adotou a Decisão-Quadro 2008/977/JAI, de 27 de Novembro de 2008, com vista a regulamentar esta matéria. Mais recentemente, esta Decisão foi

---

[13] Heraclides Dos Santos Silva, "*A Protecção de Dados Pessoais na Era Global: O Caso Schrems*", Universidade Nova de Lisboa, 2017.

[14] Comissão Europeia, Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, COM (2012) 11 final, 2012/11 (COD), Bruxelas, 25 de janeiro de 2012.

objeto de revogação com a entrada em vigor da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de crimes ou execução de sanções penais e à livre circulação desses dados.

Resumidamente, esta nova Diretiva garante o direito fundamental dos cidadãos à proteção de dados quando os dados pessoais forem utilizados pelas autoridades responsáveis na decorrência da aplicação da lei. Desta forma, auxilia-se a cooperação transfronteiriça na luta contra a criminalidade e o terrorismo, garantindo que os dados pessoais de vítimas, testemunhas e suspeitos de crimes se encontram devidamente protegidos.

Similarmente, com o intuito de acautelar eventuais situações de impunibilidade de instituições ou órgãos da União Europeia que proviessem a uma utilização e/ou tratamento de dados pessoais que infringisse as normas europeias de proteção de dados, foi estabelecido o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Outubro de 2000. Mais recentemente também este Regulamento foi objeto de revogação após a entrada em vigor do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de Outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados.

Em seguida, e com a viragem do milénio, é proclamado um instrumento fulcral nesta temática da proteção da privacidade e dos dados pessoais: a Carta dos Direitos Fundamentais da União Europeia (doravante, CDFUE ou Carta), onde se encontram reunidos todos os direitos civis, políticos, económicos e sociais dos cidadãos europeus, com a intenção subjacente de aproximar e uniformizar os direitos dos cidadãos europeus.

Proclamada em 2000, a Carta deixou de se tratar de um documento meramente político e tornou-se juridicamente vinculativa enquanto direito primário da UE com a entrada em vigor do Tratado de Lisboa, a 1 de Dezembro de 2009 (artigo 6.º, n.º 1, do Tratado da UE). Nela, além de ser garantido o respeito pela vida privada e familiar (artigo 7.º), está simultaneamente previsto o direito à proteção de dados (artigo 8.º, n.º 1), "elevando este à condição de direito fundamental no quadro do direito da EU.".

Note-se, porém, que por ter sido formulada posteriormente à data de adoção da Diretiva, o seu artigo 8.º deve ser interpretado no sentido de abranger a legislação europeia sobre proteção de dados que lhe fosse preexistente.

2.3. A REFORMA DE 2016: O RGPD

Os progressos tecnológicos e a crescente globalização trouxeram consigo alterações significativas relativamente ao modo de acesso, recolha, tratamento e utilização dos dados pessoais, assim como novas barreiras

à efetiva proteção e garantia dos mesmos. Por outro lado, a divergência na transposição das normas europeias para o direito interno pelos Estados-Membros apresentou-se como uma das maiores adversidades nesta temática. Na realidade, se atentarmos à questão mediante o recurso a uma ótica mais prática e realista, seria inconcebível que os Estados solucionassem soberanamente e por si este desencontro legislativo relativo ao nível de proteção dos dados pessoais.

Deste modo, afigurou-se necessário a criação e delineação de um instrumento jurídico que estabelecesse uma proteção uniforme e que permitisse uma "transferência transfronteiriça fácil dos dados pessoais na UE, assegurando simultaneamente a proteção efetiva de toda as pessoas singulares no conjunto da UE."[15], compelindo, assim, a União Europeia a ir mais além na sua atuação.

Assim, em Janeiro de 2012, a Comissão apresentou um pacote de reformas sobre a regulamentação da proteção de dados pessoais. A introdução deste pacote legislativo composto por uma diretiva e um regulamento previu, na sua *ratio*, a modernização do regime vigente, propondo-se a pôr termo à fragmentação normativa que se fazia sentir nos diversos Estados relativamente a esta temática e, assim, a garantir um nível de proteção de dados pessoais transversal e análogo a todos os cidadãos europeus, independentemente do Estado onde se localizassem.

Na verdade, partindo de uma análise cronológica, esta reforma legislativa tem como pano de fundo comunicações prévias da Comissão Europeia, designadamente as comunicações intituladas:

> "*Uma abordagem global da proteção de dados pessoais na União Europeia*"[16], na qual a Comissão vem alertar para a necessidade de revisão do quadro legislativo vigente devido à "rapidez dos avanços tecnológicos e da globalização", requerendo que a UE desenvolvesse uma abordagem global e uniforme que garantisse que o direito fundamental à proteção de dados fosse plenamente respeitado, intra e extraterritorialmente;
>
> "*Proteção da privacidade num mundo interligado – Um quadro europeu de proteção de dados para o século XXI*"[17], na qual a Comissão reforça os perigos contidos na evolução tecnológica e na globalização para o manuseamento e tratamento de dados pessoais, apresentando os "elementos principais da reforma do quadro legislativo da UE relativo à proteção de dados";
>
> "*Proposta de regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses da-*

---

15 Comissão Europeia, "Acordo sobre reforma da proteção de dados na UE proposta pela Comissão estimula mercado único digital", Bruxelas, 2015.

16 Comissão Europeia, COM (2010) 609 final, '*A comprehensive approach on personal data protection in the European Union*', Bruxelas, 2010.

17 Comissão Europeia, COM (2012) 9 final, '*Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century*', Bruxelas, 2012.

dos"[18], na qual a Comissão, como o próprio título indica, apresenta a primeira proposta de regulamentação incidente sobre esta matéria.

Por intermédio deste pacote legislativo almejou-se reforçar as regras internas da União Europeia e proporcionar um maior controlo aos indivíduos sobre o paradeiro e tratamento dos seus dados pessoais, nomeadamente mediante a introdução de dois instrumentos jurídicos: por um lado, a Diretiva da Proteção de Dados destinada às autoridades policiais e judiciais – já previamente referida - e, por outro lado, o RGPD.

Não obstante o RGPD ter sido adotado em abril de 2016, foi concedido aos Estados-Membros um período de dois anos de adaptação com o intuito de permitir a preparação adequada destes à efetiva entrada em vigor do instrumento – assim, o regulamento só passou a ser verdadeiramente aplicado em 25 de maio de 2018.

Porém, os impactos e consequências, diretos e indiretos, desta reforma legislativa permite-nos facilmente compreender a longa duração de tal *vacatio legis*: se procedêssemos à comparação entre os diversos Estados-Membros e considerássemos a sua díspar dinâmica tecnológica, jurídica, económica e social, tal período de adaptação demonstrar-se-ia totalmente aceitável, e até mesmo aconselhável.

De todo o modo, e, não obstante ter-se mantido uma estrutura idêntica, na comparação do novo Regulamento com a anterior Diretiva 95/46/CE algumas diferenças há a salientar.

Desde logo, o seu impacto normativo. Isto porque, nos termos do artigo 288.º do TFUE, e ao inverso da diretiva, o regulamento é um ato legislativo da União Europeia que não carece de transposição, tendo aplicabilidade direta e efeito direto no ordenamento jurídico de cada Estado-Membro da União Europeia, encontrando-se os Estados proibidos de promulgar leis que menorizem o nível de proteção estabelecido por este regulamento.

Em segundo lugar, e, não obstante os mais diversos elementos que constituem o RGPD, cumpre notar que o seu âmbito de aplicação territorial ganhou recrudescida atenção, considerando que este novo diploma alterou as regras relativas ao âmbito territorial, previstas no artigo 3.º, n. º 1 e 2, entre os diversos elementos que o constituem, especialmente em relação aos responsáveis pelo tratamento que não se encontram estabelecidos na UE.

Verdadeiramente, esta alteração do RGPD relativamente ao âmbito de aplicação territorial das políticas europeias sobrevém do eco de uma proposta das autoridades de controlo de 2010 que sugeriram um fator de conexão mais específico, que adotasse como base de incidência os destinatários

[18] Comissão Europeia, COM (2012) 11 final, '*Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*', Bruxelas, 2012.

da atividade daqueles responsáveis pelo tratamento[19]. Desta forma, entidades sediadas num país fora da União Europeia, mas que aprovisionassem bens e serviços aos cidadãos europeus, passariam a estar abrangidas pelas normas previstas no RGPD.

O avanço supra, no sentido de uma maior homogeneização do direito aplicável à proteção dos dados pessoais foi, sem sombra de dúvidas, um momento marcante para os europeus e um triunfar dos compromissos assumidos pelos princípios da União. Isto porque, finalmente, garantiu-se que empresas estrangeiras a operar no território europeu ficariam sujeitas às mesmas regras concorrenciais aplicáveis a empresas europeias, assegurando aos cidadãos europeus um nível de proteção dos direitos fundamentais estandardizado.

Já quanto ao seu âmbito de aplicação material, e nos termos do seu artigo 2.º, o RGPD aplicar-se-á a qualquer tratamento de dados pessoais, realizado por meios parcial ou totalmente automatizados ou não automatizados, sendo que no "tratamento" se englobam todas e quaisquer operações realizadas sobre os dados pessoais.

No plano principiológico, o artigo 5.º do Regulamento veio, simultaneamente, consagrar sete princípios fundamentais essenciais à proteção de dados[20], que deverão ser imperativamente observados pelos responsáveis pelo tratamento, bem como, a existir, pelos seus subcontratantes.

Ademais, os direitos individuais em matéria de proteção de dados pessoais foram igualmente reforçados. Com a introdução do RGPD, ao indivíduo titular de dados pessoais passou a ser permitido o acesso aos seus dados e a obtenção de informações mais completas, conforme o disposto no artigo 15.º.

Por outro lado, o titular dos dados passou, simultaneamente, a usufruir de um «direito ao esquecimento», nos seis casos especificados no artigo 17.º[21]. O "direito ao esquecimento" determina que ao titular dos dados pessoais seja atribuída a faculdade de solicitar a exclusão dos mesmos que lhe digam respeito, sem demora injustificada.

---

19 Graça Canto Moniz, "*Breves reflexões sobre o enquadramento normativo do Regulamento Geral de Proteção de Dados Pessoais (RGPD)*", Centro de Estudos Judiciários, Outubro de 2021.

20 A saber: princípio da licitude, lealdade e transparência, princípio da limitação das finalidades, princípio da minimização dos dados, princípio da exatidão, princípio da limitação da conservação, o princípio da integridade e confidencialidade e princípio da responsabilidade.

21 A saber: os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento (alínea a)); o titular retira o consentimento e não existe outro fundamento jurídico para o referido tratamento (alínea b)); o titular opõe-se ao tratamento e não existem interesses legítimos prevalecentes que o justifiquem (alínea c)); os dados pessoais foram tratados ilicitamente (alínea d)); os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento está sujeito (alínea e)); e os dados pessoais foram recolhidos num determinado contexto, de acordo com o artigo 8º, número 1, do RGPD.

Também o direito à portabilidade, consagrado no artigo 20.º, se tratou de um reforço dos direitos exercidos pelo titular de dados pessoais. Nos termos deste, um titular de dados passa a ter o direito de solicitar a uma empresa ou organização que devolva os dados pessoais que lhe haviam sido oferecidos e, simultaneamente, a poder solicitar a sua transferência para uma outra empresa ou organização.

Além de fortalecer os direitos dos titulares dos dados pessoais, o RGPD reforçou igualmente as obrigações dos responsáveis pelo tratamento e dos seus subcontratantes – capítulo IV do RGPD. Este reforço sentiu-se, por exemplo, em matéria de "proteção de dados desde a conceção e por defeito" (artigo 25.º), quanto à obrigação de conserva dos "registos das atividades de tratamento" (artigo 30.º), relativamente ao dever de uma "avaliação de impacto sobre a proteção de dados" nas situações em que um determinado tipo de tratamento seja suscetível de acarretar um risco elevado para os direitos das pessoas singulares (artigo 35.º), bem como, em certos casos, quanto à necessidade de "designação do encarregado da Proteção de dados" (artigo 37.º e seguintes).

Em comparação com a anterior Diretiva, se atentarmos ao Capítulo VI, é visível que as disposições sobre a independência, funções e poderes das autoridades de controlo independentes de proteção de dados da União foram definidas com maior precisão – artigo 51.º e seguintes -, sendo de salientar, no âmbito dos poderes de correção destas, a previsão explicita da possibilidade destas autoridades suspenderem uma transferência de dados pessoais para um destinatário localizado num país terceiro ou para uma organização internacional (artigo 58.º, número 2, alínea j)).

Posteriormente, com vista à efetivação e cumprimento das normas europeias de proteção de dados, o legislador europeu previu um regime de sanções harmonizado com os poderes destas autoridades nacionais de proteção de dados, habilitando-as ao emprego de sanções a empresas que infringissem as regras de proteção de dados (artigo 83.º, números 1 e 2). As coimas a aplicar pelas Autoridades Nacionais podem atingir o valor de 20 milhões de euros ou, supletivamente, 4% do volume de negócios anual total, em virtude da dimensão da empresa (artigo 83.º, número 6).

Contudo, um ponto de capital relevância no RGPD para a dissertação em apreço são as transferências de dados pessoais para países terceiros.

Estatui o princípio geral das transferências de dados pessoais para países terceiros ou organizações internacionais, constante do artigo 44.º, que as transferências só podem ser realizadas se as condições previstas no RGPD "forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional.". Neste sentido, a regra geral é a de que o RGPD veda a realização das aludidas transferências a países terceiros, ape-

nas permitindo a sua execução em casos específicos nos quais exista uma garantia de que os aludidos dados serão devidamente protegidos[22].

Assim sendo, em que situações poderá ocorrer uma transferência de dados pessoais para países terceiros ou organizações internacionais?

Nos termos do artigo 45º do RGPD, poderá uma transferência de dados pessoais para países terceiros ou organizações internacionais ser feita com base numa decisão de adequação da Comissão, "se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado.".

Por via das decisões de adequação, a Comissão avalia o nível de proteção atribuído aos dados pessoais na ordem jurídica interna de um país terceiro. Esta análise é feita mediante o recurso a elementos taxativamente enumerados, elencados no artigo 45.º, número 2, e que devem obrigatoriamente ser tidos em consideração pela Comissão aquando da sua tomada de decisão. Assim, mediante o recurso a estes parâmetros, a Comissão procede a uma avaliação global do país terceiro em apreço, "devendo ser analisada não só a existência de um quadro legal que garanta a proteção dos dados pessoais, como também a existência de autoridades que garantam a aplicação e a observância das normas de proteção dos dados, bem como a adoção de sistemas através dos quais os titulares dos dados possam fazer valer os seus direitos."[23].

Porém, e não obstante se encontrarem instituídos parâmetros para avaliar, *in casu*, a adequação do nível de proteção, nem o RGPD, nem a Diretiva 95/46/CE, desenvolveram o conceito do "nível de proteção adequado", deixando um vazio conceptual. Tal conceito veio a ser clarificado aquando do julgamento do processo C- 362/14 (*Maximillian Schrems v. Data Protection Commissioner*) - a ser analisado mais adiante. Em sede deste, o Tribunal de Justiça da União Europeia veio determinar que um "nível de proteção adequado" não poderia remeter-se à exigência de um nível de proteção idêntico àquele previsto na União Europeia, mas antes a um "nível de proteção substancialmente equivalente". Deste modo, "o objetivo não é imitar ponto por ponto a legislação europeia, mas sim estabelecer um «standard de equivalência essencial», o que pressupõe uma prévia avaliação global do sistema de proteção de dados pessoais do país terceiro, em particular ao nível das

---

22 Lucas Pires Martinho, "*Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems*", Anuário da Proteção de Dados 2018, Lisboa, CEDIS, 2018

23 Aline Chiappetta, "*Transferências Transatlânticas de Dados Pessoais na Era Pós Snowden à Luz do Regulamento Geral sobre a Proteção de Dados*", Universidade de Coimbra, 2018

garantias de proteção aplicáveis e mecanismos de supervisão e reparações disponíveis"[24].

Posteriormente a ser proferida a decisão de adequação por parte da Comissão são seguidos os trâmites habituais, como se de um Estado-Membro se tratasse. Assim, "o efeito de tal decisão consiste em permitir a livre circulação de dados pessoais para esse país terceiro sem haver necessidade de o exportador de dados apresentar outras garantias ou obter qualquer autorização."[25].

No entanto, há que salientar que do artigo 45.º, número 3, consta uma obrigação expressa no sentido de a Comissão rever periodicamente – no mínimo de quatro em quatro anos – todas as decisões de adequação previamente tomadas e que, na eventualidade de deixar de estar assegurado o nível de proteção adequado, a Comissão possui plenos poderes para alterar, suspender ou revogar a sua decisão de adequação (artigo 45.º, número 5).

Por sua vez, o artigo 46.º do RGPD determina o procedimento a adotar na falta de uma "decisão de adequação" ou nos casos em que a mesma tenha sido, posteriormente, suspensa ou revogada pela Comissão. Em situações deste tipo, as transferências passam a ficar sujeitas à prestação de garantias adequadas (por exemplo, o recurso a regras vinculativas aplicáveis às empresas, cláusulas-tipo de proteção de dados adotadas pela Comissão ou por uma autoridade de controlo, ou cláusulas contratuais autorizadas por esta autoridade). E, além destas garantias devem ainda ser concedidos aos titulares dos dados pessoais direitos oponíveis e medidas jurídicas corretivas eficazes, conforme o artigo 46.º, número 1, parte final.

Em último lugar, e apenas nas situações taxativamente previstas no RGPD, na falta de uma "decisão de adequação" ou de garantias adequadas, seria ainda possível efetuar transferências ao abrigo do artigo 49º.

Deste modo, é incontestável que a reforma do quadro legislativo da proteção de dados pessoais constituiu um instrumento essencial à implementação e desenvolvimento do Mercado Único Digital Europeu, no sentido em que, por um lado, (i) fortaleceu a segurança dos titulares de dados nas novas tecnologias de informação e, por outro lado, (ii) tem permitido à Europa manter a sua posição cimeira na economia digital mundial.

Posto isto, cumpre atentar com maior detalhe à questão das transferências de dados pessoais entre a União Europeia e os Estados Unidos.

---

[24] Cláudia Fernandes Martins, "Aprovada decisão de adequação para transferências de dados entre UE-Japão", 2019

[25] Comissão Europeia, "*Comunicação da Comissão ao Parlamento Europeu e ao Conselho, Intercâmbio e proteção de dados num mundo globalizado*", Bruxelas, 2017, COM (2017) 7 final

3. AS TRANSFERÊNCIAS DE DADOS PESSOAIS ENTRE A UNIÃO EUROPEIA E OS ESTADOS UNIDOS DA AMÉRICA

As relações entre a União Europeia e os Estados Unidos são relações solidificadas e enraizadas no tempo e na memória de todos nós. A criação da NATO, precedente à própria criação da União Europeia, e a partilha de valores e princípios estruturais, designadamente de natureza política, social, económica e de segurança, têm vindo a garantir a longevidade e a estabilidade no tempo desta relação estadual bilateral. Além do mais, há um interesse acrescido em manter a estabilidade desta relação, nomeadamente porque, de uma ótica comercial, os Estados Unidos são o maior parceiro da União Europeia, sendo que as suas economias "representam mais de 50 % do PIB mundial, 25 % das exportações mundiais e mais de 30 % das importações mundiais", e as suas relações económicas "são as mais significativas do mundo, com um comércio transatlântico total no valor de 1,09 biliões de dólares em 2014"[26].

Todavia, e não desconsiderando o exposto supra, "a forma como cada um dos dois parceiros decide fazer face, separadamente ou em conjunto, a numerosos desafios globais com que se defronta não deixará de influenciar a sua relação bilateral, mas a existência de um desacordo quanto a questões específicas não é necessariamente sinal de uma deriva na relação"[27]. E não obstante não serem residuais as matérias em que existe esse desacordo, apresenta-se aqui com especial relevância a temática das transferências de dados pessoais e, consequentemente, o seu armazenamento e tratamento.

Na atual sociedade de informação em que vivemos as transferências de dados pessoais entre os Estados Unidos e a UE apresentam-se como um assunto de capital relevância considerando que o fluxo de transferências entre estes dois blocos representa, em termos comparativos, o maior fluxo do mundo. E, note-se, este fluxo transatlântico não se restringe a transferências oriundas de acordos comerciais, mas também àquelas provenientes da contraprestação de serviços, como é o caso de dados provenientes do uso de plataformas online gratuitas, tais como o *Facebook* e o *Twitter*, bem como de plataformas e motores de pesquisa online gratuitos, tais como o *Google*, cujas sedes são, na sua grande maioria, nos Estados Unidos.

Deste modo, sem a existência de um direito europeu para sua a proteção, os dados pessoais dos cidadãos europeus seriam, *ab initio*, enviados, armazenados e tratados como se de cidadãos americanos se tratasse, não havendo qualquer diferenciação no *modus operandi* e nas regras aplicáveis

---

[26] Parlamento Europeu, Resolução do Parlamento Europeu, de 26 de maio de 2016, sobre a transferência transatlântica de dados (2016/2727(RSP)).

[27] Comunicação da Comissão Europeia ao Parlamento de 26.07.1995, "A Europa e os Estados Unidos", 1995

quando estivéssemos perante cidadãos norte-americanos *vs*. quando estivéssemos perante cidadãos europeus.

Todavia, e conforme já fora analisado, vários são os instrumentos que, assegurando um nível de proteção elevado, tornam exequíveis as transferências de dados pessoais entre a União Europeia e um país terceiro.

E porque a conjuntura americana é uma de índole inteiramente oposta à presente na conjuntura europeia, a inexistência destes instrumentos supra acarretaria que os titulares europeus de dados pessoais ficassem desprotegidos quando os seus dados fossem transferidos para o espaço extra-UE, tornando praticamente insignificante o nível de proteção dos dados pessoais e da vida privada consagrado no território europeu pelo direito europeu.

Assim, na (re)conquista e expansão de um espaço económico transatlântico "há que identificar com precisão as áreas em que é possível de uma forma realista concluir acordos bilaterais suscetíveis de remover os obstáculos existentes ou de melhorar de outra forma a atividade económica transatlântica."[28].

As notáveis dissemelhanças, não só entre a valoração liberdade *vs*. segurança, bem como entre o sistema jurídico americano e europeu no que respeita às políticas aplicáveis aos dados pessoais, inviabilizariam a emissão da referida decisão de adequação. Tal problemática motivou o Departamento de Comércio dos EUA a negociar com a Comissão Europeia o avanço de sistemas de autocertificação que, mediante a sua adesão, permitissem a livre transferência de dados pessoais entre a UE e as empresas certificadas sediadas nos EUA. "Não se tratava, por isso — e à semelhança dos países em relação aos quais já foram emitidas decisões de adequação —, de declarar que todas as transferências para os EUA eram lícitas, mas de determinar que seriam lícitas transferências para as organizações que se encontrassem certificadas através do referido mecanismo."[29].

Assim, como resultado das negociações e do avanço dos sistemas de certificação supra, proveio uma decisão de adequação por parte da Comissão Europeia: a Decisão "Porto Seguro". Esta decisão, e consequente invalidação, irá ser objeto de análise no ponto subsequente. Atente-se.

3.1. A DECISÃO DE ADEQUAÇÃO "PORTO SEGURO"

"O modelo europeu de proteção dos dados distingue-se de forma significativa do modelo americano. Enquanto o direito europeu preza por uma proteção dos dados realizada em um instrumento jurídico uniforme e harmôni-

[28] Comunicação da Comissão Europeia ao Parlamento de 26.07.1995, "A Europa e os Estados Unidos", 1995

[29] Tiago Félix Da Costa & Marta Salgado Areias, "*Breve Nota sobre o Acórdão do Tribunal de Justiça da União Europeia no Processo C-311/18 – Data Protection Commissioner Contra Facebook Ireland Limited e Maximillian Schrems («ACÓRDÃO SCHREMS II»)*", Revista de Direito e Tecnologia, VOL. 2 (2020), NO. 2.

co, nos Estados Unidos a proteção destes dados é realizada por meio da regulamentação, autorregulamentação, bem como através de leis esparsas e setoriais, sem que haja uma autoridade de controlo uniforme que garanta a aplicação dos instrumentos legais relativos à proteção dos dados."[30].

Dito isto, e não obstante os exportadores de dados pudessem lançar mão dos remanescentes instrumentos legais previstos para a realização de transferências de dados pessoais destinadas a países terceiros à UE – nomeadamente, e como já referido previamente, as garantias adicionais ou, em último caso, as derrogações previstas no artigo 26.º da Diretiva e, atualmente, no artigo 49.º do RGPD – , o clima de desconfiança e instabilidade acentuava-se, muito devido aos enormes custos associados a estas transferências e aos possíveis desfechos negativos decorrentes de uma ulterior anulação ou alteração das condições, transformando estas transferências em autênticos riscos assumidos unilateralmente por aqueles.

Assim, e conforme dito supra, para acautelar o receio fundado e legítimo por parte dos exportadores e "para limitar esta incerteza e fornecer um enquadramento mais previsível para as transferências de dados"[31], dos esforços e negociações desenvolvidos entre o Departamento de Comércio americano e as instituições europeias de 1998 a 2000 surgiu a Decisão 2000/520/CE, adotada a 26 de julho de 2000 (doravante, "Decisão" ou "Decisão Porto Seguro").

A Decisão "Porto Seguro" (ou, originalmente, *Safe Harbour Decision*), emergiu posteriormente à publicação dos pareceres do Grupo de Trabalho do artigo 29.º, e na sequência do exercício das funções de controlo prévio atribuídas ao Parlamento Europeu, que deu luz verde à sua aprovação.

Nesta medida, a Decisão veio evidenciar que, diante dois sistemas jurídicos tão dissemelhantes como eram, e ainda hoje são, o sistema jurídico americano e o sistema jurídico europeu, um *common ground* poderia, ainda assim, ser atingido com vista a possibilitar a previsão legal destas transferências e o fomento dos fluxos transatlânticos, não desvalorizando, contudo, o nível de proteção atribuído aos titulares de dados pessoais no espaço europeu.

Assim, e tendo por base os requisitos previstos no artigo 25.º da Diretiva 95/46/CE, as relações entre a União Europeia e os Estados Unidos foram aprofundadas com a decisão de adequação emitida pela Comissão Europeia em 2000, surgindo os sete Princípios de "Porto Seguro".

Segundo o princípio do Aviso, os titulares dos dados pessoais deveriam ser informados de que os seus dados estariam a ser recolhidos, o destino

---

30 Aline Chiappetta, "*Transferências Transatlânticas de Dados Pessoais na Era Pós Snowden à Luz do Regulamento Geral sobre a Proteção de Dados*", Universidade de Coimbra, 2018.

31 DECISÃO DA COMISSÃO de 26 de Julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípios de «porto seguro» e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América, Anexo I, 2000

para o qual seriam utilizados e os tipos de terceiros a quem a informação seria comunicada. A organização aderente aos princípios do "Porto Seguro" deveria ainda fornecer informações detalhadas sobre os meios como esses titulares a poderiam contactar, nomeadamente para responder a questões e/ou a reclamações.

Já conforme o princípio da Escolha, os titulares de dados pessoais deveriam ter a opção de cancelar a recolha («opt out» ou opção de não participação) e de reencaminhar a transferência dos seus dados para entidades terceiras, mediante o acesso a mecanismos claros e transparentes, facilmente disponíveis e pouco custosos.

Nos termos do princípio da Re-transferência, as transferências de dados para entidades terceiras só poderiam ocorrer para organizações que adotassem também os princípios "Porto Seguro" e cumprissem as restantes disposições da Diretiva, mediante acordo escrito que garantisse esse mesmo nível de proteção.

Seguidamente, segundo o princípio da Segurança, as organizações deveriam tomar as precauções razoáveis para evitar a perda, utilização indevida e acesso, revelação, alteração ou destruição não autorizados dos dados pessoais.

Conforme o princípio da Integridade dos Dados, os dados pessoais transferidos deveriam ser pertinentes para a finalidade para a qual haviam sido recolhidos.

Segundo o princípio do Acesso, os cidadãos deveriam poder ter acesso às informações mantidas sobre eles e corrigi-las, alterá-las ou excluí-las, caso se encontrassem imprecisas ou incorretas.

E, finalmente, nos termos do princípio da Aplicação, deveriam existir meios eficazes que garantissem o cumprimento dos princípios de «Porto Seguro», recursos para os cidadãos a que se referissem os dados, bem como consequências para as organizações em casos de violação dos princípios.

Estes princípios, quando aplicados em conformidade com as diretrizes previstas nas quinze questões mais frequentes (FAQ), confeririam um nível de proteção adequado às transferências transatlânticas de dados pessoais, permitindo-se, desta forma, o livre fluxo de informações pessoais dos Estados-Membros da UE para empresas sediadas nos EUA, equiparando-as às transferências operadas intra-UE, ou seja, abolindo quaisquer exigências adicionais.

Para tal, as empresas americanas teriam de subscrever e agir de acordo com os princípios do "Porto Seguro", mediante prévia comunicação da sua adesão ao Departamento de Comércio dos EUA ou ao seu representante (artigo 1.º, n.º 3, da Decisão). Posteriormente à análise sobre a adesão, estas entidades responsáveis deveriam publicar, no sítio web criado ad hoc para este fim específico, uma lista das organizações autocertificadas que tivessem aderido aos princípios do "Porto Seguro".

Assim, além de prestar um caráter informativo destinado a potenciais empresas e cidadãos interessados, a presença de uma organização na lista *web* do Departamento de Comércio dos EUA criava nos titulares de dados pessoais uma expetativa legítima de que os seus dados encontrar-se-iam devidamente protegidos, criando uma sensação de segurança semelhante àquela obtida, paralelamente e a título de exemplo, através de um selo de qualidade ou conformidade sujeito a constante fiscalização.

Todavia, e não obstante a adesão a este sistema de autocertificação ser voluntária, algumas condições deveriam estar necessariamente reunidas para que estas empresas pudessem receber transferências de dados ao abrigo da Decisão.

Deste modo, somente aquelas que estivessem sujeitas à jurisdição da Comissão Federal de Comércio dos EUA poderiam aderir ao sistema[32], excluindo-se, desde logo, uma panóplia de prestadores de serviços, nomeadamente nos setores das finanças e das telecomunicações.

Ademais, a organização que desejasse aderir aos princípios do "Porto Seguro" deveria agir em conformidade com esses princípios, devendo as suas políticas de proteção da vida privada serem públicas, bem como a efetiva subscrição aos princípios, garantindo uma maior transparência das suas práticas.

Além do exposto supra, o processo de autocertificação deveria ser objeto de renovação anual, cabendo novamente a análise e decisão de tal renovação à competência estatutária do Departamento de Comércio do EUA.

No entanto, a Decisão previa também o elenco de sanções a aplicar a organizações que, por não cumprirem com a aplicação prática dos princípios a que haviam previamente subscrito, encontrar-se-iam sujeitas à imputação da prática de atos desleais e artificiosos, por violarem quer o direito americano, quer o direito europeu. E, nos termos do Anexo V da Decisão, em situações de transgressão à Decisão a entidade competente para sancionar estas organizações e aplicar medidas coercivas seria a Comissão Federal de Comércio dos EUA[33].

Além do exposto supra, nos termos do artigo 3.º, n.º 1, alíneas a) e b) da Decisão, as autoridades responsáveis pela proteção dos dados pessoais de cada Estado-Membro tinham a competência para suspender as transferências dos mesmos para as organizações certificadas, especificamente quando (i) o Departamento de Comércio ou um mecanismo de recurso independente determinasse que a organização em causa não obedecia aos princípios de "Porto Seguro" ou (ii) quando existissem fortes indicativos para

---

[32] Shara Monteleone & Laura Puccio, "*From Safe Harbour to Privacy Shield - Advances and shortcomings of the new EU-US data transfer rules*", European Parliamentary Research Service, Members' Research Service, 2017

[33] Emily Jones, "*The Safety of Safe Harbor*", Journal of Direct, Data and Digital Marketing Practice, 15, 2013

supor que esses princípios não estavam a ser respeitados. Esta suspensão cessaria apenas quando o respeito pelos princípios aplicados em conformidade com as FAQ estivesse assegurado e a autoridade competente do Estado-Membro fosse de tal cessação informada.

Ademais, perante a existência de indícios de que os organismos responsáveis pela verificação do cumprimento dos princípios do "Porto Seguro" nos EUA não estivessem a desempenhar eficazmente as suas funções, poderia a Comissão informar de tal situação o Departamento de Comércio dos EUA e, se entendesse necessário, proceder à revogação ou suspensão da Decisão "Porto Seguro", assim como restringir o seu âmbito de aplicação, nos termos do artigo 3.º, n.º 4, da Decisão. Já se o nível de proteção proporcionado pelos princípios tivesse sido revogado por ulterior legislação norte-americana, poderia a Decisão ser adaptada em qualquer altura, nos termos do artigo 4.º, n.º 1, da Decisão.

Ora, tendo por base tudo o que fora dito previamente, é irrefutável a importância que a Decisão "Porto Seguro" apresentava para a economia transatlântica, quer para os particulares titulares dos dados pessoais, quer para as empresas exportadoras desses mesmos dados. Ainda assim, a sua vigência nunca foi pacífica, tendo surgido, inclusive previamente à sua entrada em vigor, inúmeras vozes de preocupação e de discórdia relativamente à questão da efetiva proteção e garantia dos dados pessoais.

As vozes de preocupação agravaram-se radicalmente em junho de 2013 aquando das revelações feitas por *Edward Snowden*. O ex-analista informático que trabalhou para a *CIA* e para a *NSA*, e que se encontra atualmente a viver na Rússia ao abrigo de asilo político desde aquela data, trouxe ao palco do debate público a existência e funcionamento de programas de vigilância em larga escala das agências de inteligência americanas *CIA* e *NSA*, tais como o "*PRISM*" e o "*UPSTREAM*". Estes programas têm como desígnio aceder aos servidores das *big tech*, tais como a *Google*, a *Microsoft* e a *Apple* (não obstante a autocertificação daquelas aos princípios do "Porto Seguro"), para proceder à colheita indiscriminada e em larga escala dos dados pessoais dos seus clientes/consumidores.

Ora, a existência e operacionalidade destes programas atentavam diretamente contra a proteção e garantia dos dados pessoais ao abrigo da Decisão, levando as mais variadas autoridades de controlo e organismos públicos e privados a questionar a amplitude do nível de proteção efetivamente garantido aos dados pessoais que estariam a ser transferidos da União Europeia para as empresas certificadas nos EUA.

Na realidade, variados *Data Protection Authorities* (DPA) vieram expressar a sua preocupação imediatamente após o escândalo, como foi o caso da DPA alemã, que já em 2010 havia alertado para a violação dos princípios do "Porto Seguro" na decorrência de políticas nacionais americanas que colidiam diretamente com a Decisão. Posteriormente às declarações de *Snowden*, a DPA de *Bremen*, "solicitou que as empresas que transferissem

dados para os EUA informassem se e como as empresas recetoras nos EUA impediriam o acesso a dados pessoais pela NSA."[34].

Também a Comissão Europeia não ficou inerte face às declarações de *Snowden*. Em novembro de 2013 veio salientar algumas insuficiências na Decisão mediante a emissão de duas declarações: a Comunicação "Restabelecer a confiança nos fluxos de dados entre a UE e os EUA" [COM(2013) 846 final], e a Comunicação "sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na EU" [COM(2013) 847 final], nas quais veio analisar as consequências para a continuidade do acordo transatlântico de transferência de dados pessoais em face da atuação do governo americano.

Na Comunicação n.º 846, logo na segunda página, a Comissão veio arguir a inadmissibilidade de tais programas, contrapondo a importância da continuidade das relações entre os EUA e a UE e o peso económico associado às transferências de dados pessoais. Posteriormente, já na página oitava, veio criticar a falta de transparência das empresas americanas autocertificadas, bem como a falta de supervisão por parte das autoridades americanas competentes.

Já com a Comunicação n.º 847, a Comissão veio analisar a fundo a Decisão "Porto Seguro", desde a sua criação até à data, baseando-se também nas informações avançadas pelo grupo de trabalho *ad hoc* UE-EUA sobre a proteção de dados, e em dois relatórios por si emitidos em 2002 e 2004 acerca da Decisão. Com base nestes documentos, veio apontar que os mecanismos de salvaguarda dos titulares de dados pessoais previstos na legislação norte-americana beneficiariam, sobretudo e quase exclusivamente, os cidadãos e residentes dos EUA, não existindo qualquer meio legal para "os titulares de dados da UE ou dos EUA obterem acesso ou solicitarem a retificação ou a supressão dos dados, ou apresentarem um recurso administrativo ou judicial caso, no âmbito de programas de vigilância dos EUA, os seus dados pessoais sejam recolhidos e tratados posteriormente".

Assim, não seria inconcebível a existência de situações em que os próprios titulares europeus dos dados pessoais não tivessem sequer conhecimento de que esses dados estariam a ser acedidos pelo governo americano para fins que a eles seriam alheios e para os quais não teriam quaisquer meios de defesa.

As incertezas acerca da continuidade da vigência da Decisão eram gritantes, o que decorria, em grande medida, das diferenças entre os dois sistemas jurídicos. A quase utópica possibilidade de se vir a encontrar, efetivamente, o tal *common ground* entre as duas potências parecia mais longe do que nunca. Isto porque "na UE, procurou-se estruturar o seu regime em torno da

---

[34] Nina Pupalova, "*Transatlantic data flow under the EU-U.S. Privacy Shield: An adequate protection of the fundamental right to protection of personal data?*", Faculdade de Direito da Universidade de Oslo, 2017

defesa dos direitos fundamentais e assentá-lo em uma estrutura jurídica uniforme que vigore em todo o espaço europeu. (...) Fundamentalmente distinto, o modelo vigente nos EUA caracteriza-se pelo foco na promoção dos fluxos de dados e pelo seu carácter fragmentado, existindo uma multiplicidade de instrumentos jurídicos que só se aplicam em determinados sectores, tipos de dados ou Estados. Tal deveu-se ao facto de a Quarta Emenda da Constituição dos EUA, que tutela a privacidade e que passou a abranger também os dados pessoais a partir de 1967 com o caso *Katz vs. United States*, já não ser suficiente para proteger o direito à privacidade dos riscos criados pelas novas tecnologias."[35]. Assim, ao privilegiar-se nos EUA o sistema da autorregulação empresarial nestas matérias, contribui-se, simultaneamente, para a incerteza jurídica nos titulares europeus de dados pessoais.

A Comissão Federal do Comércio, ciente destas debilidades associadas ao sistema legislativo americano, propôs ao Congresso dos EUA, em março de 2012, a criação de uma legislação federal única relativa à proteção dos dados pessoais, mais próxima daquela em vigor na União Europeia, com vista a alcançar uma harmonia legislativa. Todavia, e ainda que previsivelmente, tal recomendação nunca veio a ser colocada em prática pelo Governo americano.

Não obstante todas estas fragilidades e controvérsias, e até mesmo a própria noção por parte da Comissão da existência de falhas cruciais na Decisão "Porto Seguro" e de violações aos seus princípios, logo desde os primeiros anos da sua vigência, esta optou por manter o sistema em vigor, "reforçando-o", por considerar que "a sua revogação afetaria negativamente os interesses das empresas, tanto da UE como dos EUA, que são membros do sistema."[36].

Ademais, e numa nova tentativa de apaziguar as disparidades, a Comissão recomendou ainda que as políticas de proteção da vida privada das empresas autocertificadas estabelecessem se e quando a legislação americana consentia a recolha de dados transferidos ao abrigo do mecanismo da Decisão "Porto Seguro" pelas autoridades públicas americana.

Por fim, a Comissão salientou ainda que as exceções baseadas em motivos de segurança nacional somente poderiam ser invocadas mediante a verificação cumulativa de dois critérios essenciais: (i) o critério da proporcionalidade e (ii) o critério da necessidade.

Porém, numa posição diametralmente oposta àquela avançada pela Comissão Europeia, o Parlamento Europeu veio defender a suspensão do sistema de transferências de dados pessoais ao abrigo da Decisão "Porto

---

35 HERACLIDES DOS SANTOS SILVA, "*A Protecção de Dados Pessoais na Era Global: O Caso Schrems*", Universidade Nova de Lisboa, 2017

36 COMISSÃO EUROPEIA, "*Comunicação da Comissão ao Parlamento Europeu e ao Conselho - Restabelecer a confiança nos fluxos de dados entre a UE e os EUA*", COM (2013) 846 final, Bruxelas, 2011

Seguro", requerendo à Comissão a adoção de medidas que visassem garantir a proteção dos dados alojados, à data, nos EUA[37].

Tudo isto conduziu ao célebre caso de *Maximilian Schrems*, reforçando as suas pretensões. *Schrems*, advogado e ativista austríaco, foi o fundador da *ONG* "*Europe versus Facebook*", em 2011, no decurso de uma investigação académica relativa às políticas do Facebook, e principal promotor da *ONG "None Of Your Bussiness*", ambas organizações que se dedicam à investigação, identificação e divulgação de abusos e falhas nas políticas de privacidade das várias redes sociais.

No decorrer da sua investigação, *Schrems* descobriu que a sede da empresa *Facebook*, situada nos EUA, mantinha a posse e armazenamento dos dados pessoais dos seus utilizadores, inclusive aqueles pertencentes aos utilizadores europeus, transferidos ao abrigo dos princípios de "Porto Seguro". Constatou também que, segundo as suas políticas internas, o *Facebook* consentia o envio desses dados aos cidadãos europeus titulares dessas informações, mediante o exercício destes do seu direito de acesso.

Com base naquela premissa, *Schrems* avançou com um pedido à empresa norte-americana, a *Facebook Inc.,* e esta, em resposta ao pedido, enviou em formato de CD mais de 1.200 páginas, que discriminavam todos os detalhes da sua atividade naquela rede social desde a sua adesão, em 2008, inclusive aqueles que ele havia anteriormente removido, bem como conversas e contactos que havia já apagado.

Deste modo, enquanto a Comissão Europeia diligenciava no sentido de rever e reforçar a Decisão "Porto Seguro", conforme fora suprarreferido, *Maximilian Schrems*, à luz das recentes declarações de *Edward Snowden*, optou por denunciar ao *DPC* irlandês a violação dos seus direitos fundamentais, com base na atribuição a este Comissário, nos termos das suas competências estatutárias, poderes para investigar e decidir acerca da conformidade e factualidade da denúncia.

Contudo, devido a questões financeiras e de morosidade processual, entre as várias queixas que formulou (no total, vinte e três queixas), *Schrems* optou por manter apenas uma. Nos termos desta, e não obstante a sua transferência de dados ser realizada à luz da Decisão de Adequação da Comissão Europeia, *Schrems* veio arguir que os seus dados pessoais não estariam a ser alvo de uma proteção adequada nos EUA.

Sustentando-se nas alegações de *Edward Snowden* e nas políticas internas em vigor nos EUA, *Schrems* veio alegar que os dados recolhidos e transferidos pela *Facebook Ireland* para a *Facebook Inc.* poderiam ser, *a posterio-*

---

[37] PARLAMENTO EUROPEU, Resolução do Parlamento Europeu, de 12 de março de 2014, sobre o programa de vigilância da Agência Nacional de Segurança dos EUA (NSA), os organismos de vigilância em diversos Estados-Membros e o seu impacto nos direitos fundamentais dos cidadãos da UE e na cooperação transatlântica no domínio da justiça e dos assuntos internos (2013/2188(INI))

ri, requeridos por autoridades públicas americanas, tais como a *NSA, a CIA e o FBI,* ao abrigo de programas de vigilância em larga escala dessas mesmas autoridades, tais como o "*PRISM*", no qual o acesso em massa a esses dados, por razões de segurança nacional e de interesse público, e ainda que sem motivo legítimo aparente, era autorizado.

Assim, e considerando a manifesta divergência com o direito europeu, bem como a aparente inexistência de uma garantia de um nível de proteção que pudesse ser considerado adequado, *Schrems* solicitou, em junho de 2013, que fossem proibidas futuras transferências dos seus dados pessoais para a sede da empresa nos EUA, a *Facebook Inc*. Foi esta a queixa que deu origem ao processo C-362/14, que opôs *Maximillian Schrems ao Data Protection Commissioner*, mais conhecido como Acórdão *Schrems* I.

A autoridade de controlo irlandesa, por entender que não existiam provas suficientes que suportassem as alegações, arquivou o pedido de *Schrems*. Salientou ainda que as questões relacionadas com o nível de proteção dos dados pessoais garantido pelos EUA deveriam ser decididas à luz da Decisão "Porto Seguro" e que, segundo aquela decisão, a Comissão Europeia havia considerado que, efetivamente, aquele país garantia um nível de proteção adequado. Assim, o *DPC* irlandês entendeu que nada mais poderia fazer.

Todavia, inconformado com a decisão, *Schrems* interpôs recurso para o *High Court* irlandês.

Numa primeira etapa do julgamento, este tribunal procedeu à análise dos factos à luz do direito nacional, acabando por concluir que as práticas americanas eram visivelmente contrárias àquelas consagradas pela Constituição irlandesa, na qual se garante o direito ao respeito à vida privada, assim como que qualquer derrogação ou limitação deste direito deverá sempre respeitar o princípio da proporcionalidade e da necessidade.

Assim, o *High Court* veio a concluir que, caso o processo fosse julgado apenas com base no direito interno, sobre o Comissário irlandês recairia, necessariamente, a obrigação de iniciar uma investigação dos factos denunciados por *Schrems*.

Contudo, numa segunda etapa do julgamento, e por entender que "a Decisão 2000/520/CE não satisfazia os requisitos que decorriam tanto dos artigos 7.° e 8.° da CDFUE como dos princípios estabelecidos pelo Tribunal de Justiça no acórdão *Digital Rights Ireland*", o *High Court* entendeu que as questões colocadas em causa por *Schrems* deveriam ser apreciadas à luz do Direito Europeu, mais concretamente à luz dos artigos 7.º, 8.º e 47.º da CDFUE, bem como dos artigos 25.º, n.º 6, e 28.º da Diretiva 95/46/CE.

Assim, o Supremo Tribunal de Justiça irlandês optou por suspender a instância e submeter duas questões prejudiciais ao Tribunal de Justiça da União Europeia (TJUE), nomeadamente: quanto aos poderes das autoridades nacionais de controlo, na aceção do artigo 28.º da Diretiva 95/46/CE,

perante uma decisão da Comissão adotada nos termos do artigo 25.º, n.º 6, desta Diretiva; e quanto à validade da Decisão 2000/520/CE.

Ora, mediante acórdão de 6 de outubro de 2015, o TJUE veio analisar as questões prejudiciais supra colocadas pelo Supremo Tribunal de Justiça irlandês.

Assim, e relativamente à primeira questão, no âmbito de uma denúncia ao *DPC* e perante uma situação em tenha sido previamente emitida uma decisão de adequação por parte da Comissão, estará a autoridade de controlo nacional totalmente sujeita à orientação instituída na Decisão da Comissão ou, diversamente, deverá essa autoridade de controlo nacional investigar sobre a efetiva adequação do regime de proteção de dados pessoais do país terceiro?

Neste domínio, o TJUE veio desde logo relembrar que o direito europeu, mais concretamente o artigo 28.º, n.º 1, da Diretiva, exige a "instituição, nos Estados-Membros, de autoridades de controlo independentes", o que "constitui, portanto, como salienta o considerando 62 da Diretiva 95/46, um elemento essencial do respeito da proteção das pessoas relativamente ao tratamento de dados pessoais". Assim, caberá a essas mesmas autoridades de controlo a fiscalização do cumprimento do direito europeu de proteção de dados pessoais, bem como a verificação se as transferências para um país terceiro estão de acordo com os critérios avançados pela Diretiva.

E, conforme já foi dito previamente, a Comissão, no âmbito dos poderes que lhe foram atribuídos, designadamente no artigo 25.º, n.º 6, da Diretiva, poderá adotar uma decisão de adequação que, nos termos do artigo 288.º do Tratado de Funcionamento da UE, "possui caráter obrigatório para todos os Estados-Membros destinatários e impõe-se, portanto, a todos os seus órgãos (…), na medida em que tem por efeito autorizar transferências de dados pessoais dos Estados-Membros para o país terceiro visado pela mesma.", sendo que nos órgãos vinculados à decisão emitida pela Comissão encontram-se, efetivamente, as autoridade de controlo.

Logo, "enquanto a decisão da Comissão não for declarada inválida pelo Tribunal de Justiça, os Estados-Membros e os seus órgãos, entre os quais se encontram as autoridades de controlo independentes, não podem adotar medidas contrárias a essa decisão, tais como atos destinados a constatar, com efeitos vinculativos, que o país terceiro visado pela referida decisão não assegura um nível de proteção adequado.". Esta decisão gozava, pois, de uma presunção de legalidade.

Contudo, seria impensável que os poderes das autoridades de controlo pudessem ser restringidos pela existência de uma decisão de adequação, sob pena de estarmos perante uma atuação por parte da Comissão que excede as suas competências, além de que os poderes das autoridades de controlo estão garantidos, quer pela Carta e pelo TFUE, quer pelo artigo 28.º da Diretiva. De igual modo, seria analogamente inconcebível que uma decisão de adequação da Comissão impedisse "as pessoas cujos dados pessoais tenham sido ou possam ser transferidos para um país terceiro de

apresentarem às autoridades nacionais de controlo um pedido, nos termos do artigo 28.º, n.º 4, desta diretiva, relativo à proteção dos seus direitos e liberdades no que diz respeito ao tratamento desses dados", sob pena de estarmos perante uma limitação ilegítima do leque de direitos dos indivíduos.

Por conseguinte, propugnou o TJUE que as autoridades de controlo deveriam investigar e decidir, com toda a diligência necessária, as denúncias respeitantes à proteção dos direitos e liberdades fundamentais de um titular de dados pessoais, inclusivamente perante uma situação de transferência para um país terceiro ao qual haja sido, previamente, emitido uma decisão de adequação. Aliás, um entendimento diverso a este seria, incontestavelmente, um entendimento *contra legem*.

Posteriormente à fase de investigação, poder-se-ia estar perante um, de dois cenários: caso a autoridade de controlo entendesse que a reclamação era infundada, deveria arquivá-la e informar o queixoso das vias de recurso jurisdicionais e administrativas remanescentes a que pudesse ter direito; na situação oposta, em que entendesse que a denúncia teria fundamento, deveria remeter a questão para os órgãos jurisdicionais nacionais e invocar perante estes toda a argumentação que considerasse válida e seriam estes, caso assim o entendessem, que remeteriam a questão, a título prejudicial, para o TJUE. Isto porque "o Tribunal de Justiça é o único competente para declarar a invalidade de um ato da União, como uma decisão da Comissão adotada nos termos do artigo 25.º, n.º 6, da Diretiva 95/46, tendo a exclusividade desta competência por objeto garantir a segurança jurídica, preservando a aplicação uniforme do direito da União.".

Assim, em suma, o TJUE veio responder à primeira questão prejudicial da seguinte forma:

> "O artigo 25.º,n.º 6, da Diretiva 95/46/CE [...] lido à luz dos artigos 7.°, 8.° e 47.° da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que uma decisão adotada ao abrigo desta disposição, como a Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46 relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ), emitidos pelo Department of Commerce dos Estados Unidos da América, através da qual a Comissão Europeia constata que um país terceiro assegura um nível de proteção adequado, não obsta a que uma autoridade de controlo de um Estado-Membro, na aceção do artigo 28.º desta diretiva, conforme alterada, examine o pedido de uma pessoa relativo à proteção dos seus direitos e liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que foram transferidos de um Estado-Membro para esse país terceiro, quando essa pessoa alega que o direito e as práticas em vigor neste último não asseguram um nível de proteção adequado."

Conforme foi abordado previamente, o TJUE é o órgão competente para declarar a validade ou invalidade dos atos da União. Assim, ele prosseguiu para a análise da validade da Decisão de Adequação 2000/520/CE, à luz da Diretiva 95/46/CE e da Carta.

Para tal, o TJUE começou por contextualizar o enquadramento jurídico no qual iria basear a sua decisão, realizando uma análise do artigo 25.º da Diretiva, nos termos do qual as transferências de dados pessoais para um país terceiro só poderiam ser realizadas se esse país terceiro assegurasse um nível de proteção adequado.

Porém, já foi referido que a Diretiva não avançou com um conceito do que seria, na prática, esse nível de proteção adequado, elencando apenas os critérios a ter em consideração na avaliação desse país – a sua legislação interna, os seus compromissos internacionais, bem como as suas práticas, valores e costumes.

De todo o modo, entendeu o TJUE que "para alcançar este nível de adequação, a ordem jurídica do país terceiro não precisa ser idêntica, mas sim substancialmente equivalente à consagrada na UE"[38], exigindo-se, tão-só, que os meios judiciais usados por esse país fossem eficazes ao ponto de garantirem uma proteção substancialmente equivalente àquela que estaria garantida dentro da União Europeia. Ademais, e considerando que a conjuntura de um país não é estática, mas antes dinâmica, encontrando-se sujeita a uma intrínseca evolução e desenvolvimento, considerou-se que a análise dos critérios supra não deveria ser uma análise feita isoladamente no tempo, mas sim uma que estaria sujeita a constante reavaliação periódica. Os desenvolvimentos do país terceiro, fossem eles sociais, económicos, políticos ou legais, deveriam ser tidos em consideração pela Comissão no momento da reavaliação da Decisão de Adequação.

Assim, e em suma, o TJUE entendeu que a Comissão deveria averiguar periodicamente se a adequação do nível de proteção dos dados do país terceiro se continuaria "a justificar de facto e de direito" e que "tal verificação impõe-se, em qualquer caso, quando haja indícios que suscitem dúvidas a este respeito.".

Com base no exposto supra, o TJUE passou, seguidamente, a examinar a adequação do nível de proteção dos dados pessoais transferidos para os EUA tendo por base a Decisão "Porto Seguro". Para tal considerou as disposições da Decisão 2000/520/CE, lidas à luz dos artigos relevantes da Diretiva 95/46/CE e da CDFUE, como também a evolução legislativa americana no âmbito da proteção de dados, tendo vindo destacar os seguintes pontos:

> Qualificou o sistema consagrado na Decisão como sendo um de autorregulação, exortando a necessidade de serem desenvolvidos mecanismos de fiscalização e de punição de qualquer violação das normas destinadas à proteção dos direitos fundamentais;

[38] Aline Chiappetta, "*Transferências Transatlânticas de Dados Pessoais na Era Pós Snowden à Luz do Regulamento Geral sobre a Proteção de Dados*", Universidade de Coimbra, 2018.

> Constatou que os princípios de "Porto Seguro" apenas seriam aplicáveis às empresas norte-americanas autocertificadas que recebessem dados pessoais de cidadãos europeus ou residentes na União Europeia, estando excluído do seu âmbito de aplicação as autoridades públicas americanas;
>
> Realçou que na Decisão "Porto Seguro" não se encontravam referências suficientes aos meios como os EUA garantiriam, efetivamente, um nível de proteção adequado, quer por força da sua legislação interna, quer por força dos compromissos internacionais assumidos, conforme estipulava o artigo 25.º da Diretiva 95/46/CE;
>
> Destacou que o Anexo I da Decisão permitia a limitação – quase arbitrária – da aplicação dos princípios de "Porto Seguro", nomeadamente por motivos de segurança nacional, de interesse público e de execução da lei, o que determinaria, por um lado, que as organizações norte-americanas autocertificadas ficariam sujeitas à vontade dessas autoridades públicas americanas e, por outro lado, que caso a legislação americana fosse contrária aos princípios de "Porto Seguro" as organizações deveriam privilegiar a aplicação da lei americana, por força da consagração do princípio do primado no direito americano;
>
> Alertou para a eventualidade de que, devido à ausência de critérios delimitadores do acesso e posterior utilização das autoridades públicas americanas dos dados pessoais, estas autoridades poderiam aceder a esses dados e atribuir-lhes um tratamento e um fim manifestamente distinto daquele que havia justificado a sua transferência em primeiro lugar;
>
> Verificou que os titulares dos dados pessoais não eram devidamente informados sobre a utilização dos seus dados para fins diversos daqueles para os quais haviam sido recolhidos;
>
> E, por fim, considerou que a vigilância em massa operada pelas agências de segurança americanas era claramente incompatível com o quadro europeu de proteção de dados, na medida em que violava direitos fundamentais previstos na CDFUE, nomeadamente o artigo 7.º e 8.º, bem como o artigo 47.º.

Deste modo, e face ao exposto supra, o TJUE decidiu invalidar o artigo 1.º da Decisão "Porto Seguro", entendendo que a Comissão havia falhado na avaliação à adequação garantida pelos EUA, alertando para a existência de lacunas na avaliação da legislação interna e dos compromissos internacionais dos EUA.

Por fim, e já no plano das competências das autoridades nacionais de controlo, o TJUE verificou que a Decisão 2000/520/CE obstava a que aquelas autoridades exercessem as suas competências, previstas no artigo 28.º da Diretiva 95/46/CE, na medida em que o artigo 3.º, n.º 1, da Decisão determinava que aquelas autoridades poderiam aplicar as medidas necessárias para garantir o cumprimento das disposições nacionais adotadas em execução da diretiva em questão, salvo as medidas destinadas a garantir a observância do artigo 25.º da Diretiva.

Contudo, o artigo 25.º, n.º 6, da Diretiva não atribuiu à Comissão qualquer competência para limitar os poderes das autoridades nacionais de controlo, até porque estas deveriam gozar de plena independência e dos poderes necessários para investigar e decidir as denúncias efetuadas pelos titulares de dados pessoais. Assim, o TJUE invalidou igualmente o artigo 3.º da Decisão.

Deste modo, em consequência das apreciações feitas no acórdão e atendendo ao facto de que os artigos 1.º e 3.º da Decisão, invalidados pelo TJUE, seriam indissociáveis dos artigos 2.º e 4.º da Decisão, o TJUE declarou, em 6 de outubro de 2015, a invalidade absoluta da Decisão 2000/520/CE, mais conhecida por *Safe Harbour Decision.*

Cumpre, assim, atentar às consequências desta invalidação pelo TJUE da Decisão "Porto Seguro".

O Grupo de Trabalho do artigo 29.º, que agrupava as 28 autoridades nacionais de proteção de dados, bem como a Autoridade Europeia para a Proteção de Dados (AEPD), emitiu, a 16 de outubro de 2015, uma declaração relativamente aos efeitos práticos do acórdão[39]. Em primeiro lugar, apelou à necessidade de um maior diálogo entre os Estados-Membros e as instituições europeias com as autoridades norte-americanas, de modo que fossem encontradas novas soluções para as transferências transatlânticas de dados.

Na medida em que a invalidação da Decisão "Porto Seguro" determinou a impossibilidade de os exportadores de dados recorrerem aos mecanismos nela previstos, o Grupo de Trabalho avançou também com a enunciação e esclarecimento dos instrumentos jurídicos alternativos a usar nas transferências de dados, nomeadamente as cláusulas contratuais-tipo de proteção de dados (CCT) e as regras vinculativas para empresas.

Além disso, e na eventualidade de que não ser encontrada nenhuma solução para o futuro com as autoridades norte-americanas, asseverou também que as autoridades de proteção de dados deveriam ser diligentes e adotar todas as medidas necessárias e apropriadas.

Todavia, também a Comissão não ficou inerte com o sucedido e, tendo em vista facilitar o uso de tais instrumentos nas transferências internacionais, aprovou, em conformidade com o artigo 26.º, n.º 4, da Diretiva, quatro conjuntos de cláusulas contratuais-tipo respeitadoras dos requisitos do artigo 26.º, n.º 2, da Diretiva: duas referentes a transferências entre responsáveis pelo tratamento de dados, e duas referentes a transferências entre um responsável pelo tratamento de dados e um subcontratante, em que cada uma estabelecia as obrigações respetivas dos exportadores e dos importadores de dados[40].

Além disso, e após examinar as vantagens e desvantagens de cada um dos instrumentos alternativos disponíveis, a Comissão reiterou a premência na elaboração de um novo quadro para as transferências transatlânticas de da-

---

39 Grupo De Trabalho Do Art. 29.º, "*Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)*", Bruxelas, 2015.

40 Comunicação Da Comissão Ao Parlamento Europeu E Ao Conselho sobre a transferência de dados pessoais da UE para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na sequência do acórdão proferido pelo Tribunal de Justiça no processo C-362/14 (Schrems), Bruxelas, 6.11.2015, COM (2015) 566 final.

dos pessoais, considerando ser essa a via de atuação que melhor garantiria a prossecução da proteção dos direitos fundamentais dos cidadãos europeus.

Por outro lado, "a decisão do TJUE em apreço estabeleceu ainda novos critérios de apreciação do nível de protecção conferido pelo país terceiro aos dados pessoais, que deverão ser seguidos pela Comissão quando adoptar uma decisão nos termos do art. 25.º, n.º 2 e n.º 6, da Directiva. Esses novos requisitos são, aliás, semelhantes àqueles que estão previstos no art. 41.º, n.º 2, da proposta de Regulamento (art. 45.º, n.º 2, do Regulamento aprovado), ao ponto de parecer que o TJUE os teve em consideração quando tomou a sua decisão."[41]. Assim, nos termos destes novos critérios, na análise das leis internas de um país terceiro, deveria a Comissão verificar, forçosamente, a existência de normas que autorizassem possíveis ingerências nos direitos fundamentais dos particulares, inclusive aquelas que tivessem por base motivos de segurança nacional e o interesse público[42].

Porém, a principal consequência prática do acórdão do TJUE foi a de que o *High Court* irlandês deveria ordenar o Comissário irlandês a proceder à análise da denúncia efetuada por *Schrems* e que determinasse se seria, ou não, necessário suspender as transferências de dados pessoais, com base no facto de o país não oferecer um nível de proteção adequado. Na realidade, tal veio efetivamente a suceder, a 20 de outubro de 2015, em sede de audiência final do processo no órgão jurisdicional irlandês.

Não surpreendentemente, na sequência do Acórdão *Schrems* I, o *Facebook* veio emitir novas declarações, alegando que com a invalidação da Decisão "Porto Seguro" as suas transferências de dados pessoais tinham passado a ser realizadas com base nas cláusulas-tipo de proteção de dados ao abrigo da Decisão 2010/87/UE (as CCT). Ora, com base nestas declarações, *Schrems* reformulou o conteúdo da sua queixa, contestando que as transferências assentes nas cláusulas contratuais-tipo, tal como sucedia com o regime de "Porto Seguro", não garantiriam o nível de proteção adequado, sendo incompatíveis com os níveis de proteção vigentes no direito da União, e reiterando que o acesso infundado e manifestamente desproporcionado aos dados pessoais de cidadãos e residentes europeus pelas autoridades públicas norte-americanas se mantinha, apelando, por estes motivos à sua suspensão ou proibição.

A 24 de maio de 2016, o Comissário irlandês veio apresentar as suas conclusões provisórias fruto da sua investigação. Nestas, concluiu pela existência de um risco fundado de os dados pessoais serem consultados nos EUA de forma incompatível com os artigos 7.º e 8.º da Carta. Simultaneamente, entendeu também o Comissário que não estavam igualmente disponíveis

---

41 Heraclides Dos Santos Silva, "*A Protecção de Dados Pessoais na Era Global: O Caso Schrems*", Universidade Nova de Lisboa, 2017

42 Domingos Soares Farinho, *"(Un)Safe Harbour: Comentário à Decisão do TJUE C-362/14 e suas Consequências Legais*", Fórum de Proteção de Dados, n.º 2, 2016.

as vias de recurso compatíveis com o artigo 47.º da Carta. E, por fim, considerou que as cláusulas-tipo de proteção de dados (CCT) não permitiam evitar esses riscos, acabando por remeter um pedido de reenvio prejudicial ao TJUE – o acórdão *Schrems* II, a ser analisado de seguida.

3.2. A DECISÃO DE ADEQUAÇÃO "ESCUDO DE PROTEÇÃO DA PRIVACIDADE"

A declaração de invalidade da Decisão de Adequação "Porto Seguro" veio abalar o comércio das transferências transatlânticas, deixando as organizações americanas num clima de medo e insegurança relativamente ao futuro. Por este motivo, e pela importância atribuída ao mercado das transferências entre estas duas potências, ecoou um sentimento de urgência na negociação entre a Comissão e o Departamento de Comércio americano, para a criação de um novo *framework* que regulasse novamente a migração transatlântica dos dados pessoais.

Após alguns meses de negociações, a Comissão Europeia divulgou o esboço do novo Escudo de Proteção da Privacidade (originalmente, "*EU-US Privacy Shield*"). O projeto, bem como os textos que originaram a sua criação, foram tornados públicos a 29 de fevereiro de 2016[43]. Simultaneamente, a Comissão divulgou ainda uma comunicação[44] onde resumia as alterações realizadas para garantir a eficiência deste novo mecanismo, em evidente harmonia com os objetivos afirmados nas Orientações Políticas da Comissão *Juncker*[45].

Assim, e conforme ditam os trâmites procedimentais vigentes na União Europeia, posteriormente à conclusão das negociações, incumbiu à Comissão a apresentação do novo acordo ao Grupo de Trabalho do artigo 29.º. Isto porque, este órgão consultivo europeu independente em matéria de proteção de dados, tal como a AEPD, devem ser consultados antes da tomada da deliberação final pelo Colégio dos Comissários, com o intuito de se pronunciarem acerca do nível de proteção prognosticado.

O Grupo de Trabalho do artigo 29.º, no parecer que emitiu em abril de 2016[46], enalteceu vários aspetos do acordo alcançado entre as duas potências, considerando, desde logo, que o novo quadro legal colmatava algumas das lacunas presentes no *framework* anterior, nomeadamente no âmbito do desenvolvimento efetuado no campo principiológico, na previsão da in-

---

43 Comissão Europeia, Comunicado de imprensa "*Restabelecer a confiança nas transferências transatlânticas de dados através de sólidas garantias: Comissão Europeia apresenta Escudo de Privacidade UE-EUA*", Bruxelas, 2016.

44 Comissão Europeia, "*Comunicação da Comissão ao Parlamento Europeu e ao Conselho - Transferência transatlântica de dados: restaurar a confiança através de garantias sólidas*", COM (2016) 117 final, Bruxelas, 2016.

45 Jean-Claude Juncker, "*Um novo começo para a Europa: o meu Programa para o emprego, o crescimento, a equidade e a mudança democrática*", Estrasburgo, 2014.

46 Grupo De Trabalho Do Art. 29.º, "*Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*", Working Paper 238, Bruxelas, 2016.

cumbência de avaliações periódicas, na previsão de novos mecanismos de supervisão, bem como do reforço das garantias legais para os cidadãos e residentes europeus.

Todavia, o Grupo de Trabalho alertou para a subsistência da possibilidade de condutas abusivas por parte das autoridades públicas americanas, que continuavam a ter o poder de aceder aos dados pessoais transferidos ao abrigo do novo quadro legal.

Seguidamente, alertou também para a crescente burocratização do *framework*, considerando que tal característica determinaria uma maior dificuldade no acesso à informação por parte dos particulares.

Ademais, o Grupo de Trabalho entendeu também existir uma complexidade acrescida no acesso aos novos mecanismos de recurso, exortando a necessidade da emissão de esclarecimentos acerca dos procedimentos a adotar.

Um ponto de maior relevo neste parecer foi a chamada de atenção para a figura do mediador (o *Ombudsman*) e para a extensão – ou, no caso, carência – dos seus poderes de investigação. Não obstante a ideia de que este novo mecanismo traria vantagens e benefícios aos cidadãos europeus, o Grupo de Trabalho ficou com dúvidas relativamente à sua independência e imparcialidade, considerando que se trataria de um cargo que seria exercido por um vice-secretário do Departamento de Estado americano, a ser nomeado pelo Presidente dos EUA e confirmado pelo Senado.

Já a Autoridade Europeia para a Proteção de Dados (AEPD), enquanto organismo independente de orientação das instituições europeias sobre matérias relativas ao tratamento de dados pessoais, adotou uma abordagem mais ríspida. No seu parecer[47] começou, desde logo, por afirmar a necessidade de se proceder a uma alteração do acordo, por considerar que aquele não abarcava as salvaguardas necessárias para proteger os direitos fundamentais dos cidadãos europeus. Ademais, tal como o Grupo de Trabalho do artigo 29º, advertiu para a facilidade no acesso aos dados pessoais por parte das autoridades públicas norte-americanas, o que poderia contribuir, à semelhança da decisão invalidada, para situações de ingerência indiscriminada e excessiva por parte daquelas autoridades a dados de titulares europeus.

"Porém, a observação mais pertinente da AEPD sobre o acordo alcançado foi referente ao acesso por razões de segurança nacional aos dados transferidos: enquanto a Decisão "Porto Seguro" tratava formalmente essa hipótese como uma excepção, o "Escudo de Protecção da Privacidade EU-EUA" parece indicar, pela atenção que dedica, que o acesso e análise dos dados pessoais, transferidos para fins comerciais, por parte dos serviços de segurança norte-americanos corre o risco de se tornar uma prática frequen-

[47] Autoridade Europeia Para a Protecção De Dados, "*Opinion 4/2016 - Opinion on the EU-U.S. Privacy Shield draft adequacy decision*", Bruxelas, 2016.

te."[48], alertando, consequentemente, para uma possível eventual declaração de invalidade do novo quadro legislativo.

Também o Parlamento Europeu se pronunciou sobre a matéria. Após as sessões plenárias de 25 e 26 de maio de 2016, nas quais se debateu o conteúdo e prosperidade do novo *framework*, salientou-se que a existência de uma solução estável para o quadro das transferências transatlânticas teria, necessariamente, de estar em sintonia com o respeito aos direitos à proteção de dados e à vida privada garantidos pelo direito da União Europeia.

Assim, e em suma, as críticas encetadas ao acolhimento deste novo quadro legislativo não tinham sido propriamente favoráveis. Tal deveu-se, maioritariamente, à aparência de um compromisso frugal por parte dos EUA e pela persistência de situações de ingerência em larga escala por parte das autoridades de vigilância americanas. Nesta medida, aliás, um ponto de extrema relevância há a ressalvar: posteriormente ao Acórdão *Schrems* e à queda do sistema *Safe Harbour*, as práticas de espionagem e vigilância norte-americanas não só se mantiveram, como os seus poderes de vigilância foram até expandidos através de vários instrumentos legais, nomeadamente a Secção 702 do *FISA* (*Foreign Intelligence Surveillance Act*) e a *Executive Order* n.º 12333 – a ser analisados mais adiante.

Todavia, o "Escudo de Proteção da Privacidade UE-EUA" foi adotado, em 12 de julho de 2016, entrando de imediato em vigor no espaço europeu, ao passo que no território americano, foi a publicação no *U.S. Federal Register*[49], o jornal oficial do governo federal norte-americano, que determinou que as empresas que pretendessem recorrer ao novo *framework* poderiam começar o seu processo de autocertificação a partir do dia 1 de agosto, junto do Departamento de Comércio dos EUA, ao qual competiria analisar a candidatura.

Paralelamente, de modo a atenuar a complexidade do novo sistema jurídico, por um lado, a Comissão publicou um guia com orientações dirigidas aos cidadãos europeus que pretendessem recorrer aos mecanismos de recurso disponíveis no novo acordo e, por outro lado, o Departamento de Comércio e a *International Trade Administration* (ITA) lançaram um *website* com informações dirigidas a particulares e a empresas que pudessem ser pertinentes.

Ora, inegável é concluir que existiam semelhanças consideráveis entre o mecanismo do "Porto Seguro" e o mecanismo do "Escudo de Proteção da Privacidade". Atentemos a estas características individualmente.

Em primeiro lugar, quanto ao método de adesão (i): ambos os mecanismos se traduziam em sistemas de autocertificação por meio do qual as or-

---

48 Heraclides Dos Santos Silva, "*A Protecção de Dados Pessoais na Era Global: O Caso Schrems*", Universidade Nova de Lisboa, 2017.

49 International Trade Administration, Department Of Commerce, "*Notice of Availability of Privacy Shield Framework Documents*", Federal Register, Vol. 81, n. º 148, Office of the Federal Register, 2016.

ganizações declaravam, anualmente, a sua adesão aos princípios previstos no Anexo II da Decisão de Execução 2016/1250, da Comissão Europeia.

Ademais, tal como na decisão anterior, também a adesão aos princípios do "*Privacy Shield*" era voluntária. No entanto, e em segundo lugar, estes eram vinculativos (ii). Assim, à semelhança do mecanismo anterior, a partir do momento em que a entidade subscrevesse os princípios, ela ficaria igualmente vinculada às regras constantes da nova decisão, ficando também sujeita aos poderes das autoridades americanas encarregues pela administração e supervisão do cumprimento dos princípios.

Todavia, em comparação com a decisão anterior, estes poderes e mecanismos de supervisão e administração foram ampliados (iii). Com a entrada em vigor da nova Decisão, o Departamento de Comércio dos EUA passou a ter uma maior capacidade de supervisão e fiscalização, bem como a ser responsável não só pela elaboração, como também pela atualização, da lista das organizações autocertificadas.

Além disso, foram atribuídos poderes de investigação e de execução à Comissão Federal do Comércio. Assim, a esta incumbia dar "prioridade às queixas de incumprimento dos princípios de privacidade submetidas por organismos independentes de resolução de litígios ou de autorregulação, pelo *Department of Commerce* e pelas APD (por iniciativa própria ou após a receção de queixas) a fim de determinar se a secção 5 da *FTC Act* (lei relativa à Comissão reguladora do comércio federal) foi violada.".

Já no âmbito da limitação do acesso aos dados pessoais transferidos ao abrigo da "*Privacy Shield*" (iv) por parte das autoridades públicas norte-americanas, e como forma de apaziguar as preocupações sentidas em toda a Europa, os EUA passariam a estar vinculados ao critério da necessidade, assim como às limitações e garantias legais estabelecidas, nomeadamente: na *Executive Order* 12333 (*EO*1233); na *Presidential Policy Directive 28* (*PPD*-28); e No *Foreign Intelligence Surveillance Act – FISA*.

Segundo uma publicação emitida em maio de 2017, sob o título "Procedimentos de implementação sob a Diretiva de Política Presidencial-28, Atividades de Inteligência de Sinais (PPD-28)", a "PPD-28 reforça as práticas atuais, estabelece novos princípios e fortalece a supervisão, para garantir que na condução de inteligência de sinais (SIGINT), os Estados Unidos levam em consideração não apenas as necessidades de segurança da nossa nação e dos nossos aliados, mas também a privacidade das pessoas ao redor do mundo."[50].

Assim, de acordo com a *PPD*-28, a recolha de informações pessoais deveria ter como fundamento a lei ou uma autorização presidencial, além de que devia ser processada de acordo com as normas previstas na Constituição (mais especificamente, a Quarta Emenda) e remanescente legislação ameri-

[50] "*Implementing Procedures under Presidential Policy Directive-28, Signals Intelligence Activities*" (PPD-28), 2017.

cana, sem nunca descurar o respeito pela privacidade e dignidade do titular dos dados pessoais em causa.

"Por seu turno, a secção 702 do *FISA* autoriza as autoridades americanas a coletar dados de cidadãos de países terceiros que estejam localizados fora do território dos EUA, com a assistência obrigatória dos fornecedores de serviços de comunicações eletrônicas dos EUA, para fins de coleta de "informações de inteligência no estrangeiro". O *FISA* é a base legal para programas de vigilância como o *PRISM* e o UPSTREAM, ambos detalhados pelas revelações de *Snowden*."[51].

Por fim, a *Executive Order* n.º 12333, de 1981, traduziu-se num decreto executivo destinado a ampliar os poderes e responsabilidades das agências de inteligência dos EUA, tendo sido considerada pela comunidade de inteligência americana como um documento fundamental que possibilitou a expansão das atividades de recolha de dados. É com base nesta que, por exemplo, "a *NSA* coleta, retém, analisa e divulga informações de inteligência de sinais estrangeiros.".

Ademais, na nova Decisão é estabelecida a regra da seletividade (v), isto é, a regra de que as recolhas de dados devem ser, sempre que possível, seletivas, o que determina que "a recolha em larga escala só será autorizada quando a recolha seletiva através da utilização de discriminantes (…) não possa realizar-se por motivos técnicos ou operacionais".

Nestes casos supra, a recolha em larga escala passa a ser admitida. Porém, "a «utilização» posterior de tais dados através do acesso é estritamente limitada a objetivos de segurança nacional específicos e legítimos (…)", entre os quais a luta contra o terrorismo, a luta contra a proliferação, a detenção e combate a determinadas atividades de potências estrangeiras, a cibersegurança, a detenção e combate a ameaças para os EUA e os seus aliados e o combate às ameaças criminosas transnacionais.

Com o novo acordo, também novas vias de recurso (vi) que garantissem uma proteção mais abrangente dos direitos dos cidadãos europeus foram instituídas. Assim, às organizações responsáveis pelo tratamento de dados passou a ser exigido que as queixas que lhes fossem apresentadas obtivessem uma resposta no prazo máximo de 45 dias.

Foi também exigido às organizações que diligenciassem no sentido de "informar claramente as pessoas sobre um ponto de contacto, interno ou externo à organização, que procederá ao tratamento das queixas (nomeadamente qualquer estabelecimento competente na União que possa responder a questões e queixas) e sobre os mecanismos independentes de tratamento das queixas.".

---

[51] Aline Chiappetta, "Transferências Transatlânticas de Dados Pessoais na Era Pós Snowden à Luz do Regulamento Geral sobre a Proteção de Dados", Universidade de Coimbra, 2018.

Ademais, os cidadãos europeus poderiam também recorrer a um organismo independente, sediado nos EUA ou na EU, que seria designado pela organização, criado especificamente para a resolução de litígios.

Posteriormente, esgotadas as vias de recurso disponíveis, mas entendendo o titular dos dados que a sua queixa não tinha sido devidamente resolvida, poderia este requerer uma arbitragem vinculativa ao abrigo do Comité do "*Privacy Shield*", na qual poderia escolher dois a três árbitros, com base numa lista elaborada pelo Departamento do Comércio dos EUA e pela Comissão Europeia.

Além do exposto supra, uma das principais novidades do novo *framework* foi a instituição de um Mediador para o Escudo de Proteção da Privacidade (o *Ombudsman*) (vii). John Kerry, à data Secretário de Estado, assumiu o compromisso de criar este mecanismo de supervisão das situações de ingerência, cujas funções seriam desempenhadas por um membro do Departamento de Estado, e a quem poderiam os governos estrangeiros "expressar preocupações sobre as atividades de informação de origem eletromagnética dos EUA.". Enquanto órgão independente, a este Mediador caberia analisar as queixas individuais que lhe fossem enviadas pelos titulares de dados pessoais que, por algum motivo, tivessem razões para acreditar que tinham sofrido uma ingerência abusiva pelas agências de segurança nacional norte-americanas.

Posteriormente à fase de investigação, o Mediador deveria decidir se tinha, ou não, existido uma violação da lei e, cumulativamente, indicar a forma de sanação da mesma. Posteriormente, deveria certificar se o incumprimento tinha sido corrigido, sendo que, no exercício das suas funções o Mediador poderia requerer a cooperação de outros mecanismos de supervisão, o que asseguraria "o acesso aos conhecimentos especializados necessários".

Ademais, também a obrigação de um reexame periódico anual da verificação da adequação (viii) foi previsto com a entrada em vigor do "Escudo de Proteção da Privacidade EU-EUA", tal como havia sido solicitado pelo TJUE no seu acórdão Schrems I. Assim, sobre a Comissão recairia a obrigação de uma reapreciação anual do "Escudo de Proteção da Privacidade UE-EUA", a ser feita conjuntamente com o Departamento de Comércio e com a Comissão Federal do Comércio dos EUA, "acompanhados, se adequado, de outros departamentos e serviços envolvidos na aplicação das disposições do Escudo de Proteção da Privacidade (…).". Em suma, deveria a Comissão certificar-se, periodicamente, se se mantinham factual e legalmente justificados os fundamentos dos quais provinham a decisão de adequação.

Note-se, porém, que nas situações em que a Comissão recebesse informações que pudessem colocar essa adequação em causa, a obrigação de averiguação supra tornava-se obrigatória.

Para auxiliar este procedimento de averiguação, impendeu sobre os EUA a responsabilidade de informar a Comissão sobre eventuais alterações legislativas, quer no domínio da proteção dos dados pessoais, quer no domínio

das limitações e garantias aplicáveis ao acesso das autoridades públicas a esses mesmos dados.

Do procedimento de reexame supra resultaria a elaboração de um relatório público sobre os resultados da reapreciação, que deveria ser objeto de apresentação ao Parlamento Europeu e ao Conselho.

Ademais, tal como no sistema "Porto Seguro", também na "Privacy Shield" foram consagrados, e em alguns casos aprofundados, os princípios (ix)[52]:

> do aviso, que se traduz na "obrigação por parte das empresas certificadas de fornecerem informações chave relacionadas com o processamento de dados pessoais aos respetivos titulares";
>
> da escolha, que "confere aos titulares dos dados o direito de se oporem ao tratamento";
>
> da responsabilização pela transferência ulterior (anteriormente, princípio da re-transferência), que estabelece que "qualquer transferência de dados pessoais de uma empresa para um responsável pelo tratamento ou um subcontratante, independentemente de este se encontrar nos EUA ou num país terceiro (fora dos EUA e/ou da UE), só é possível para fins específicos e limitados.";
>
> da segurança, nos termos do qual "as empresas que processam dados pessoais devem implementar medidas de segurança adequadas, as quais devem ter em consideração os riscos relacionados com o processamento em si e com a categoria de dados processados.";
>
> da integridade dos dados e limitação dos fins (anteriormente, princípio da integridade dos dados), segundo o qual "os dados pessoais só podem ser conservados enquanto a sua utilização esteja conforme a finalidade do tratamento (…)";
>
> do acesso, nos termos do qual "os titulares dos dados têm o direito de obter a confirmação, por parte das empresas, de que os seus dados pessoais estão a ser processados, bem como o direito a que estes lhes sejam comunicados sem demora injustificada.", assim como o direito a "alterar ou eliminar informações pessoais sempre que estas estejam incorretas ou tenham sido tratadas em violação dos princípios.";
>
> e do recurso, aplicação e responsabilidade (anteriormente, princípio do recurso), que "determina que as empresas certificadas devem proporcionar mecanismos que assegurem a conformidade com os sete princípios do *Privacy Shield* e também formas de recurso (…).".

Além destes princípios, teriam ainda de ser respeitados os "princípios suplementares", emitidos pelo *Department of Commerce* dos EUA, entre os quais: os princípios referentes aos dados sensíveis, às exceções jornalísticas, à responsabilidade subsidiária, à realização de auditorias e auditorias jurídicas, ao papel das autoridades responsáveis pela proteção dos dados, aos dados relativos a recursos humanos, à resolução de litígios e aplicação, entre outros.

---

[52] CATARINA CONDE NOGUEIRA, "*PRIVACY SHIELD vs. ACÓRDÃO C-311/18 - "SCHREMS II*"", CiberLaw by CIJIC, EDIÇÃO N.º XI – MARÇO DE 2021

Ora, como já foi exposto supra, a Comissão Europeia, na tentativa de assegurar a *compliance* entre a legislação americana e a lei europeia, bem como a existência de um nível de proteção adequado na transferência transatlântica de dados, publicou a Decisão de Adequação (UE) 2016/1250, a 12 de julho de 2016.

Porém, poucas não foram as dúvidas existentes relativamente à sua conformidade com as exigências previstas pela lei europeia, principalmente após a entrada em vigor do RGPD. Aliás, a própria AEPD já tinha alertado, no seu parecer de maio de 2016 para a existência de hesitações quanto à compatibilidade da Decisão de Adequação com os requisitos previstos pelo, entretanto em vigor, RGPD, que veio aplicar-se "ao tratamento de dados pessoais efetuado no âmbito das atividades de empresas ou entidades com sucursais estabelecidas na UE, independentemente do local onde os dados são efetivamente processados, bem como ao tratamento de dados pessoais de titulares residentes na UE, efetuado por empresas constituídas fora da UE que ofereçam bens ou serviços a esses titulares ou qualquer tratamento relacionado com o controlo do comportamento destes"[53].

De todo o modo, e não obstante a sua vigência tumultuosa, a Decisão "*Privacy Shield UE-EUA*", manteve-se válida aproximadamente 4 anos e somente a 16 de julho de 2020 veio o Tribunal de Justiça da UE declará-la inválida, numa decisão que ficou conhecida como *Schrems* II, e que veio, assim, comprovar o persistente cenário de divergência entre os dois sistemas jurídicos nas matérias da privacidade e da proteção de dados. Mas como é que se chegou a esta invalidação por parte do TJUE?

Quando *Schrems* foi convidado a reformular a sua queixa, devido à *Facebook Inc.* ter alegado que, com a invalidação da Decisão "Porto Seguro", as transferências de dados pessoais por si executadas passaram a ser realizadas ao abrigo das cláusulas-tipo de proteção de dados, previstas na Decisão 2010/87/UE. Deste modo, na queixa reformulada, *Schrems* manteve a tese de que os EUA não assegurariam uma proteção eficaz dos dados transferidos, sendo a sua legislação interna incompatível com os níveis de proteção vigentes na legislação europeia, tendo solicitado ao Comissário irlandês a suspensão ou proibição das transferências dos seus dados pessoais.

O Comissário irlandês, por considerar que a decisão relativamente à queixa de *Schrems* estaria dependente da validade da Diretiva 2010/87/UE, remeteu a questão para o *High Court* irlandês com vista a que este submetesse um pedido de reenvio prejudicial ao Tribunal de Justiça da UE. Estamos, assim, no âmbito do acórdão *Schrems* II.

Neste processo foram apresentadas onze questões prejudiciais ao Tribunal de Justiça da UE, as quais podem ser agrupadas e sintetizadas em três grandes questões: Quanto à aplicabilidade do RGPD nas transferências

---

53 Catarina Conde Nogueira, "*PRIVACY SHIELD vs. ACÓRDÃO C-311/18 - "SCHREMS II*"", CiberLaw by CIJIC, EDIÇÃO N.º XI – MARÇO DE 2021.

de dados pessoais baseadas nas cláusulas-tipo de proteção (que figuram na Decisão 2010/87); quanto ao nível de proteção exigido pelo RGPD no âmbito de uma transferência de dados pessoais para países terceiros; e quanto às obrigações que cabem às autoridades de controlo neste contexto.

A análise destas questões levantou, consequentemente, a questão da validade da Diretiva 2010/87, mas também da Decisão 2016/1250.

Relativamente à primeira questão, "o órgão jurisdicional de reenvio pretende saber, em substância, se o artigo 2.º, n.º 1, e o artigo 2.º, n.º 2, alíneas a), b) e d), do RGPD, lidos em conjugação com o artigo 4.º, n.º 2, TUE, devem ser interpretados no sentido de que está abrangida pelo âmbito de aplicação deste regulamento uma transferência de dados pessoais efetuada por um operador económico estabelecido num Estado-Membro para outro operador económico estabelecido num país terceiro, quando, durante ou na sequência dessa transferência, esses dados são suscetíveis de ser tratados pelas autoridades desse país terceiro para efeitos de segurança pública, de defesa e de segurança do Estado.".

Relativamente à disposição do artigo 4.º, n.º 2, do Tratado da UE, esta prevê que a segurança nacional na UE é da exclusiva responsabilidade de cada Estado-Membro. Assim, trata-se de uma disposição que respeita unicamente aos Estados-Membros, razão pela qual o TJUE concluiu que a norma não seria pertinente, no caso, para interpretar os artigos do RGPD. De todo o modo, o artigo 2.º, n.º 1, do RGPD, prevê o seu âmbito de aplicação material. E se, simultaneamente, considerarmos o conceito de "tratamento", previsto no artigo 4.º do Regulamento, a operação que consiste na transferência de dados pessoais de um Estado-Membro para um país terceiro constitui, enquanto tal, um tratamento de dados pessoais na aceção do artigo 4.º, n.º 2, do RGPD. Ademais, sendo o tratamento efetuado no território de um Estado- Membro, então só podemos concluir que o RGPD é aplicável por força do seu artigo 2.º, n.º 1.

Além disso, uma vez que a transferência de dados pessoais no processo em causa é efetuada entre duas pessoas coletivas (*Facebook Ireland e Facebook Inc*.), ela não está abrangida por nenhuma das exceções elencadas no número 2 do artigo suprarreferido.

Assim, o TJUE veio entender que, nos termos do RGPD, qualquer transferência de dados pessoais, no âmbito de uma atividade comercial, efetuada por um operador económico estabelecido num Estado-Membro para outro operador estabelecido num país terceiro não poderia "escapar ao âmbito de aplicação do RGPD pelo facto de os dados em causa serem suscetíveis de ser tratados, no decurso ou na sequência dessa transferência, pelas autoridades do país terceiro em causa, para efeitos de segurança pública, de defesa e de segurança do Estado.".

Relativamente à segunda questão, "o órgão jurisdicional de reenvio interroga o Tribunal de Justiça, em substância, sobre o nível de proteção exigido pelo artigo 46.º, n.º 1, e pelo artigo 46.º, n.º 2, alínea c), do RGPD no âmbito de uma transferência de dados pessoais para um país terceiro com base nas cláusulas- tipo

de proteção de dados. Em particular, este órgão jurisdicional pede ao Tribunal de Justiça que precise os elementos a tomar em consideração para determinar se esse nível de proteção é assegurado no contexto dessa transferência.".

Relativamente ao nível de proteção exigido para essas transferências, a leitura conjugada do artigo 46.º, n.º 1 e 2, alínea c), permite-nos concluir que caso a Comissão Europeia não tenha tomado uma decisão de adequação, nos termos do artigo 45.º, n.º 3, do RGPD, essas transferências só são exequíveis caso os responsáveis pelo tratamento ou o subcontratante tenham "apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes", inclusive quando essas garantias resultem de adoção de cláusulas-tipo de proteção adotadas pela Comissão, nos termos do n.º 2, alínea c) do artigo supra. E a natureza destas exigências, ainda que não especificada, deve ser lida à luz do artigo 44.º, sob a epígrafe "Princípio Geral das Transferências", que enuncia a regra de que nunca pode ser colocado em causa o nível de proteção das pessoas singulares.

Assim, independentemente do artigo com base no qual seja efetuada uma transferência de dados pessoais para um país terceiro, esse nível de proteção adequado tem sempre de estar garantido.

Na mesma linha de raciocínio veio o TJUE afirmar que os requisitos do RGPD sobre as "garantias adequadas, os direitos oponíveis e as medidas jurídicas corretivas eficazes, (…) devem assegurar que os direitos das pessoas cujos dados pessoais são transferidos para um país terceiro com base em cláusulas-tipo de proteção de dados beneficiam de um nível de proteção substancialmente equivalente ao garantido na União por este regulamento, lido à luz da Carta.".

Mais adiante, veio ainda abordar os elementos a tomar em consideração para determinar se esse nível de proteção é assegurado no contexto dessa transferência. Ora, embora o artigo 46.º, n.º 2, alínea c), do RGPD, não enumere os elementos a ter em conta para avaliar o caráter adequado do nível de proteção, o artigo 46.º, n.º 1, determina que os titulares dos dados devem beneficiar de garantias adequadas e gozar de direitos oponíveis e de medidas jurídicas corretivas eficazes.

Assim, para o TJUE, no contexto dessas transferências dever-se-á ter em consideração, por exemplo, "as estipulações contratuais acordadas entre o responsável pelo tratamento ou o seu subcontratante estabelecidos na União e o destinatário da transferência estabelecido no país terceiro em causa como, no que respeita a um eventual acesso das autoridades públicas desse país terceiro aos dados pessoais assim transferidos, os elementos pertinentes do sistema jurídico deste país terceiro, nomeadamente os enunciados no artigo 45.º, n.º 2, do referido regulamento.".

Por fim, "o órgão jurisdicional de reenvio pretende saber, em substância, se o artigo 58.º, n.º 2, alíneas f) e j), do RGPD deve ser interpretado no sentido de que a autoridade de controlo competente está obrigada a suspender

ou a proibir uma transferência de dados pessoais para um país terceiro com base em cláusulas- tipo de proteção de dados adotadas pela Comissão, se essa autoridade de controlo considerar que essas cláusulas não são ou não podem ser respeitadas nesse país terceiro e que a proteção dos dados transferidos exigida pelo direito da União, em particular pelos artigos 45.º e 46.º do RGPD e pela Carta, não pode ser assegurada, ou no sentido de que o exercício desses poderes está limitado a situações excecionais.".

Já havia sido mencionado no Acórdão *Schrems* I que os poderes das autoridades de controlo têm como limite o respeito de uma decisão de adequação da Comissão, nos termos do artigo 45.º, n.º 1, do RGPD, e que, por força do artigo 288.º do TFUE, essa decisão possui caráter obrigatório, o que determina que enquanto não for declarada inválida pelo Tribunal de Justiça, ninguém, inclusive as autoridades de controlo, poderá adotar medidas contrárias a essa decisão, nomeadamente a suspensão ou a proibição dessas transferências. Porém, uma situação deste tipo não pode impedir um titular de dados lesado ou potencialmente lesado de apresentar, nos termos do artigo 77.º, n.º 1, do RGPD, à autoridade nacional de controlo competente, uma reclamação relativa à proteção dos seus direitos e liberdades no que diz respeito ao tratamento desses dados. Assim, mesmo perante uma decisão de adequação da Comissão, a autoridade nacional de controlo deve poder examinar e decidir, com total independência, se a transferência desses dados respeita as exigências estabelecidas pelo RGPD e, não sendo caso disso, deve poder remeter a questão para o órgão jurisdicional nacional competente para que este, caso partilhe das dúvidas quanto à validade da decisão de adequação, proceda a um reenvio prejudicial para o TJUE para efeitos de apreciação dessa validade.

Deste modo, nos termos do artigo 51.º, n.º 1, do RGPD, as autoridades nacionais de controlo estão sempre encarregues de fiscalizar o cumprimento das regras da União relativas à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais. Deste modo, sobre elas recairá a competência para verificar se uma transferência para um país terceiro respeita as exigências impostas pelo Regulamento.

Assim, e em suma, o TJUE veio responder à questão da seguinte forma:

> "(…) o artigo 58.º, n.º 2, alíneas f) e j), do RGPD deve ser interpretado no sentido de que, a menos que exista uma decisão de adequação validamente adotada pela Comissão, a autoridade de controlo competente está obrigada a suspender ou a proibir uma transferência de dados para um país terceiro com base em cláusulas-tipo de proteção de dados adotadas pela Comissão, se essa autoridade de controlo considerar, à luz de todas as circunstâncias específicas dessa transferência, que essas cláusulas não são ou não podem ser respeitadas nesse país terceiro e que a proteção dos dados transferidos exigida pelo direito da União, em particular pelos artigos 45.º e 46.º do RGPD e pela Carta, não pode ser assegurada por outros meios, no caso de o responsável pelo tratamento ou o seu subcontratante estabelecidos na União não terem eles próprios suspendido ou posto termo à transferência.".

Da análise da sétima e da décima primeira questões prejudiciais, a validade da Diretiva 2010/87 foi, indiretamente, questionada, à luz dos artigos 7.º, 8.º e 47.º da Carta, colocando-se "a questão de saber se uma decisão da Comissão relativa a cláusulas-tipo de proteção de dados, adotada com base no artigo 46.º, n.º 2, alínea c), do RGPD, é inválida, caso não existam nessa decisão garantias oponíveis às autoridades públicas dos países terceiros para os quais os dados pessoais são ou poderiam ser transferidos com base nessas cláusulas.".

Ora, o artigo 1.º desta Diretiva dispõe que as cláusulas-tipo de proteção de dados que figuram no seu anexo oferecem garantias adequadas de proteção da vida privada, bem como dos direitos e liberdades fundamentais das pessoas. Todavia, embora essas cláusulas sejam vinculativas para as partes, é pacífico que as mesmas não são suscetíveis de vincular as autoridades desse país terceiro. E isto pode conduzir a que, quando o direito desse país terceiro o permita (como é o caso do quadro normativo dos EUA), as autoridades públicas desse país tenham à sua disponibilidade os meios legais que lhes permitam ingerir nos direitos dos titulares dos dados sem o consentimento destes.

Todavia, o Tribunal de Justiça veio dizer que, por oposição à decisão de adequação adotada pela Comissão ao abrigo do artigo 45.º do RGPD, estas cláusulas-tipo de proteção visam unicamente fornecer, aos responsáveis, garantias contratuais que se apliquem de maneira uniforme em todos os países terceiros e, como tal, independentemente do nível de proteção garantido em cada um deles. Por este mesmo motivo, pode até ser necessário, em função da situação existente em determinado país terceiro, a adoção de medidas suplementares por parte dos responsáveis pelo tratamento, a fim de assegurar o respeito desse nível de proteção que, caso não sejam consideradas suficientes, determinam a suspensão ou o término da transferência.

Assim, o Tribunal de Justiça concluiu que a Diretiva "prevê mecanismos efetivos que permitem, na prática, assegurar que a transferência de dados pessoais para um país terceiro com base nas cláusulas-tipo de proteção de dados que figuram no anexo desta decisão seja suspensa ou proibida quando o destinatário da transferência não respeite as referidas cláusulas ou esteja impossibilitado de as respeitar" e, portanto, o seu exame "à luz dos artigos 7.º, 8.º e 47.º da Carta não revelou nenhum elemento suscetível de afetar a validade desta decisão.".

Por último, também a questão da validade da Decisão 2016/1250 surgiu e foi "alvo de investigação face aos requisitos do RGPD, lidos à luz das disposições da Carta dos Direitos Fundamentais da União Europeia."[54], porque tal como a Decisão *Safe Harbour*, também a Decisão *Privacy Shield* levantava questões relativas à possibilidade de ingerência das autoridades norte-

[54] Catarina Conde Nogueira, "*PRIVACY SHIELD vs. ACÓRDÃO C-311/18 - "SCHREMS II*"", CiberLaw by CIJIC, EDIÇÃO N.º XI – MARÇO DE 2021.

americanas e consequente violação de direitos fundamentais dos titulares de dados europeus, nomeadamente aqueles relativos ao respeito da vida privada, à proteção dos dados pessoais e à proteção jurisdicional efetiva.

O TJUE considerou que "a regulamentação interna dos EUA, no que diz respeito ao acesso e utilização dos dados pessoais provenientes da UE pelas autoridades públicas americanas, resulta numa grave fragilidade na proteção adequada dos dados e seus titulares, pelo que a exigência do nível de proteção "equivalente" ao garantido na UE não é satisfeita, na medida em que os programas de vigilância levados a cabo com base nessa regulamentação não são limitados ao estritamente necessário"[55]. Entendeu também que o mecanismo do Mediador para o Escudo de Proteção da Privacidade não apresentava "nenhuma via de recurso num órgão, que ofereça às pessoas cujos dados são transferidos para os Estados Unidos garantias substancialmente equivalentes às exigidas no artigo 47.º da Carta" e, num momento marcante para o direito europeu sobre a proteção de dados pessoais, o TJUE veio invalidar a Decisão "*Privacy Shield*".

Ora, ao analisar-se o acórdão *Schrems* II, é inevitável a conclusão de que o *modus operandi* do TJUE não se revela uma surpresa, no sentido em que ele tem mantido uma atuação em consonância com a recente jurisprudência europeia em matéria de privacidade, que se fundamenta, sobretudo, numa ideia de que a tecnologia se deverá subjugar ao Direito, e não o inverso. Na realidade, este entendimento supra tem marcado presença nos mais diversos acórdãos e pareceres do TJUE, a saber:

Em 2014, no Acórdão *Digital Rights Ireland*, o TJUE declarou inválida a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações;

Em 2016, no acórdão *Tele2 Sverige vs. Tom Watson*, o Tribunal de Justiça impôs limitações às normas de detenção de dados pessoais previstos pelos governos dos EM, insurgindo-se contra "uma regulamentação nacional que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica.";

Em 2017, o Tribunal de Justiça emitiu um parecer negativo referente ao projeto de acordo entre o Canadá e a União Europeia por entender que deveriam ser previstas regras mais exigentes, na medida em que o projeto de acordo não excluía "a transferência de dados sensíveis da União para o Canadá nem a utilização e a conservação desses dados".

---

[55] Catarina Conde Nogueira, "*PRIVACY SHIELD vs. ACÓRDÃO C-311/18 - "SCHREMS II*"", CiberLaw by CIJIC, EDIÇÃO N.º XI – MARÇO DE 2021.

Por outro lado, contudo, parece afigurar-se que a decisão do TJUE em não invalidar as cláusulas contratuais-gerais, decidindo positivamente pela adequação do nível de proteção garantido por estas, se prendeu com uma vontade de não gerar um limbo jurídico relativamente às transferências EUA-UE e, consequentemente, de salvaguardar a reputação e a posição europeia no âmbito das migrações de dados pessoais. Contudo, não deixa de a tornar uma decisão, no mínimo, controversa, no sentido em que os artigos 45.º e 46.º do RGPD se aplicam quer às decisões de adequação da Comissão Europeia, quer às cláusulas contratuais-tipo. E se o assim é, resta-nos questionar o fundamento para esta diferença de tratamento face àqueles dois mecanismos de transferências de dados. Aliás, concordantemente aponta NOGUEIRA, ao afirmar que "se o *Privacy Shield* foi considerado inválido com base na incompatibilidade entre o direito da UE e a legislação de segurança norte-americana, seria expectável que as SCC estabelecidas para regular a transferência de dados precisamente para os EUA também teria a mesma consequência jurídica."[56].

E verdadeiramente, o TJUE dá enfase à crítica supra quando avança que "em qualquer caso, atendendo ao artigo 49.º do RGPD, a anulação de uma decisão de adequação como a Decisão BPD não é suscetível de criar tal vazio jurídico. Com efeito, este artigo estabelece, de forma precisa, as condições em que as transferências de dados pessoais para países terceiros podem ocorrer na falta de uma decisão de adequação ao abrigo do artigo 45.º, n.º 3, do referido regulamento ou de garantias adequadas nos termos do artigo 46.º do mesmo regulamento.", esbatendo a ideia de que as derrogações específicas deveriam ter na sua base de aplicação uma vocação de casualidade.

Todavia, e não obstante as críticas que poderiam ser adjudicadas à atuação paradoxal do TJUE, ponto assente na matéria é o de que, com o Acórdão *Schrems* II, todas as empresas cujas transferências para os EUA fossem fundadas na Decisão *Privacy Shield* deveriam passar a adotar outros instrumentos e garantias de adequação, com efeito imediato. Neste sentido, as transferências de dados pessoais de cidadãos e residentes europeus para organizações sediadas nos EUA continuou a ser possível, já não ao abrigo da Decisão, mas através: das cláusulas contratuais-tipos (CCT), das regras vinculativas aplicáveis às empresas ou, excecionalmente, por meio das derrogações previstas no artigo 49.º do RGPD.

Tendo presente esta nova realidade e com vista a facilitar a adaptação dos exportadores, a *European Data Protection Board* (EDPB) emitiu uma recomendação, na qual contemplou uma lista enunciativa de sugestões dirigida às organizações exportadoras de dados, entre os quais: conhecerem as transferências que estão a efetuar; identificarem os instrumentos de transferência utilizados; avaliarem a eficiência do instrumento de transferência

---

[56] Catarina Conde Nogueira, "*PRIVACY SHIELD vs. ACÓRDÃO C-311/18 - "SCHREMS II*"", CiberLaw by CIJIC, EDIÇÃO N.º XI – MARÇO DE 2021.

do artigo 46.º do RGPD utilizado tendo em conta todas as circunstâncias da transferência; adotarem medidas complementares; as etapas do processo a seguir quando identificavam medidas complementares eficazes; e reavaliarem as transferências frequentemente.

Porém, após uma breve análise da parte concernente às recomendações relativas à adoção de medidas suplementares eficazes, algumas dúvidas começam a surgir. Nos termos destas, as transferências devem ser imediatamente interrompidas caso não fosse possível encontrar uma medida suplementar que corrigisse eventuais lacunas, o que transmite uma ideia de que uma transferência para um país terceiro que não tenha por base uma decisão de adequação seria dificilmente aceite enquanto transferência válida, mantendo-se a questão da sua validade num eterno limbo jurídico, sendo que os riscos continuariam a correr unilateralmente para o lado do exportador. Aliás, "claramente, a orientação emitida pela *EDPB* é complexa, representando um enorme desafio para as empresas da UE, as quais estão perante uma tarefa quase impossível - encontrar soluções que permitam manter o padrão de proteção de dados da UE, independentemente do país destinatário, num mundo global em que os direitos, as leis e as normas divergem consideravelmente."[57].

Pelo exposto supra, é inevitável não concluirmos num sentido oposto ao decidido pelo Tribunal de Justiça. A decisão proveniente do julgamento *Schrems* II, é uma que se considera necessariamente suscetível de gerar um limbo jurídico ou, pelo menos, um nível inaceitável de incerteza jurídica relativamente ao futuro das transferências transatlânticas de dados pessoais. Aliás, a manifesta complexidade na adoção dos instrumentos legais alternativos pode, eventualmente, conduzir a situações de impossibilidade temporária, ou até permanente, de transferir dados para determinados países terceiros, o que determina, por um lado, (i) que acabamos por estar a reportar para o futuro um problema que já é atual e, por outro lado, (ii) que os efeitos jurídicos nefastos desta decisão se estendem além das relações EUA-UE.

4. CONSIDERAÇÕES FINAIS

Com base no exposto supra, é possível entendermos o impacto – social, económico e político – que o mercado dos dados pessoais tem na atual sociedade de informação. E se, por um lado, é verdade que se trata de um mercado relativamente recente, não deixa de ser indiscutível, por outro lado, a atual amplitude e dimensão do seu valor, diferenciando-o de qualquer outro mercado de bens ou serviços.

---

57 Catarina Conde Nogueira, "*PRIVACY SHIELD vs. ACÓRDÃO C-311/18 - "SCHREMS II*"", CiberLaw by CIJIC, EDIÇÃO N.º XI – MARÇO DE 2021.

Inicialmente, partindo da análise do quadro normativo europeu para a proteção de dados pessoais, inferimos que a regulamentação das questões da privacidade e da proteção de dados têm sido alvo de uma patente evolução no espaço europeu. A União Europeia, através dos seus vários órgãos, tem vindo a encetar esforços no sentido de promover a regulamentação do direito à privacidade e à proteção dos dados pessoais. E se nos seus primórdios este se tratou de um processo moroso, hoje podemos afirmar que vivemos num bloco regional com uma legislação coerente e contemporânea em matéria de privacidade, que coloca a tónica nos direitos fundamentais dos cidadãos.

Por conseguinte, o reforço das legislações vigentes por parte dos órgãos europeus e dos governos nacionais de cada Estado-Membro, bem como as lutas travadas pelo TJUE nestas matérias, têm permitido estabelecer na UE uma fasquia elevada de proteção, garantindo aos titulares europeus de dados pessoais uma expetativa de tutela jurídica que, como se pôde analisar ao longo da jurisprudência *Schrems*, não tem paralelo nos EUA. Aliás, como vimos, inversamente ao que sucede na União Europeia, nos EUA não é sequer reconhecido um direito fundamental à proteção de dados pessoais.

Seguidamente, procurou desenvolver-se um estudo mediante o qual fosse abordado o plano normativo para as transferências transatlânticas de dados pessoais, nomeadamente mediante o escrutínio das decisões de adequação da Comissão – as Decisões *Safe Harbour e Privacy Shield* -, bem como das suas dificuldades que conduziram, consequentemente, à sua invalidação por parte do TJUE. Deste modo, fruto das incongruências legislativas e dos compromissos frugais por parte do Governo dos EUA, o TJUE acabou por, como seria expectável, decidir de forma coincidente com o *High Court* irlandês, impactando de forma abrupta a regulamentação das transferências transatlânticas de dados pessoais em prol de um bem maior: a garantia e proteção dos direitos fundamentais.

Assim, e não obstante os esforços conjuntos, por parte dos EUA e da UE, em conceber um quadro jurídico que refletisse as exigências atuais em matéria de proteção de dados, terminamos no mesmo ponto onde iniciámos: na inexistência de um quadro normativo. Este panorama decorre, nitidamente, da dificuldade em alcançar uma regulamentação que concilie, por um lado, os interesses económicos das duas potências e, por outro lado, a proteção adequada dos dados pessoais e da privacidade dos cidadãos europeus nos dois lados do Atlântico.

Ora, tendo em consideração o exposto supra, tudo o que nos restaria interrogar seria: tendo presente o passado, qual o futuro para a regulamentação das transferências transatlânticas? Considerando as diversas fragilidades encontradas, é expectável que um novo acordo de princípio bilateral entre os EUA e a União Europeia tenha o mesmo fim trágico de que padeceram os seus antecessores. Porém, não deveremos – nem poderemos - continuar a anuir que uma matéria global, com efeitos diretos e indiretos sobre todo e cada um de nós, continue a ser tratada numa ótica bilateral,

em detrimento de avançar com instrumentos multilaterais, como é o caso da Convenção 108+, que permitam alcançar uma segurança e estabilidade jurídica cuja validade não seja questionada a cada quatro ou cinco anos. Na realidade, o mundo em que vivemos é um mundo cada vez mais global, sem fronteiras digitais, e é esta inexistência de fronteiras no mundo digital que tornam fundamental a criação de um quadro jurídico uniforme e estável, que nos torne aptos a olhar para o mundo digital atual e para os atores da cena internacional de uma forma diametralmente oposta àquela que tem vindo a ser habitual até hoje.

5. BIBLIOGRAFIA

Bennett, J. Colin, "Regulating Privacy: Data Protection and Public Policy in the Europe and the United States", in Cornell University Press; 1992.

Borchardt, Klaus-Dieter, "O ABC do direito da União Europeia", 2016. Disponível em: https://publications.europa.eu/fr/publication-detail/-/publication/f8d9b32e-6a03-4137-9e5a- 9bbaba7d1d40 (último acesso em 17.02.2022).

Calvão, Filipa Urbano, "A protecção de dados pessoais na internet: desenvolvimentos recentes", in Revista de Direito Intelectual, 2015/2.

Canto Moniz, Graça, "Breves reflexões sobre o enquadramento normativo do Regulamento Geral de Proteção de Dados Pessoais (RGPD)", in Centro de Estudos Judiciários, Outubro de 2021.

Chiappetta, Aline, "Transferências Transatlânticas de Dados Pessoais na Era Pós-Snowden à Luz do Regulamento Geral sobre a Proteção de Dados", Universidade de Coimbra; 2018.

Europe Versus Facebook, "Rapid Press Update: Facebook & NSA-Surveillance: Following "Safe Harbor" decision, Irish Data Protection Commissioner to bring EU-US data flows before CJEU again", in Europe versus Facebook, 25 de Maio de 2016, 2.ª versão, disponível em http://www.europe-v-facebook.org/PA_MCs.pdf (último acesso em 08.07.2022).

Farinho, Domingos Soares, "(Un)Safe Harbour: Comentário à Decisão do TJUE C-362/14 e suas Consequências Legais", in Fórum de Proteção de Dados, n.º 2, Janeiro de 2016.

Félix Da Costa, Tiago, Salgado Areias, Marta, "Breve Nota sobre o Acórdão do Tribunal de Justiça da União Europeia no Processo C-311/18 – Data Protection Commissioner Contra Facebook Ireland Limited e Maximillian Schrems («ACÓRDÃO SCHREMS II»)", in Revista de Direito e Tecnologia, VOL. 2 (2020), NO. 2, disponível em https://blook.pt/publications/publication/69842eb73fa6/ (último acesso em 04.07.2022).

Fernandes Martins, Cláudia; "Aprovada decisão de adequação para transferências de dados entre UE-Japão", in Macedo Vitorino & Associados, Sociedade De Advogados, R.L., 24 de janeiro de 2019, disponível em: https://www.macedovitorino.com/xms/files/20190124- Decisao_de_Adequacao_UE-Japao.pdf (último acesso em 20.06.2022).

Hustinx, Peter, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", 2014, disponível em https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection- law-review-directive_en (último acesso em 14.03.2022).

Jones, Emily, "The Safety of Safe Harbor», in Journal of Direct, Data and Digital Marketing Practice, 2013, disponível em: https://link.springer.com/content/pdf/10.1057/dddmp.2013.68.pdf (último acesso em 06.07.2022).

Kuneva, MegleNA, "Personal data is the new oil of the internet and the new currency of the digital world.", in Roundtable on Online Data Collection, Targeting and Profiling", Bruxelas, 31 de março de 2009, disponível em https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156 (último acesso em 16.02.2022).

Martinho, Lucas Pires, "Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems", in Anuário da Proteção de Dados, CEDIS, Lisboa, 2018.

Menezes Cordeiro, António, "Direito da Proteção de Dados - À luz do RGPD e da Lei n.º 58/2019", Editora Almedina, 2020

Monteleone, Shara, Puccio, Laura, "From Safe Harbour to Privacy Shield - Advances and shortcomings of the new EU-US data transfer rules", in European Parliamentary Research Service, 2017, disponível em: https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf (último acesso em 06.07.2022).

Nogueira, Catarina Conde, "PRIVACY SHIELD vs. ACÓRDÃO C-311/18 - "SCHREMS II"", in CiberLaw by CIJIC, EDIÇÃO N.º XI – MARÇO DE 2021, disponível em https://www.cijic.org/wp-content/uploads/2021/04/vf_3_Catarina-Nogueira_Privacy-Shield-vs.- Acordao-C-311_18_Schrems-II.pdf (último acesso em 10.07.2022).

Pupalova, Nina, "Transatlantic data flow under the EU-U.S. Privacy Shield: An adequate protection of the fundamental right to protection of personal data?", Faculdade de Direito da Universidade de Oslo, 2017.

Santos Silva, Heraclides, "A Protecção de Dados Pessoais na Era Global: O Caso Schrems", Universidade Nova de Lisboa, 2017.

Saxberg, Natasha, "Homo digitalis: How the human needs support digital behavior for people, organizations and societies", in Copenhagen, Dansk Psykologisk Forlag, 2015, disponível em https://revistas.uminho.pt/index.php/unio (último acesso em 21.02.2022).

Silveira, Alessandra & Froufe, Pedro, "Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos", in UNIO EU Law Journal, Vol. 4, No. 2, Julho 2018. Disponível em: https://revistas.uminho.pt/index.php/unio (último acesso em 21.02.2022).

OS DADOS PESSOAIS COMO CONTRAPRESTAÇÃO NOS CONTRATOS DE CONSUMO – A NECESSIDADE PARA A EXECUÇÃO DO CONTRATO COMO FUNDAMENTO DE LICITUDE DO TRATAMENTO

Rui Filipe Gordete Almeida

Resumo: Uma parte substancial da economia digital assenta, hoje, em fornecimentos (de conteúdos e serviços digitais) tendo por "moeda de troca" não qualquer valor pecuniário, mas sim o fornecimento de dados pessoais. Essas relações de consumo, que o consumidor médio perceciona como "gratuitas", foram recentemente reconhecidas e enquadradas no direito do consumidor: por um lado, na Diretiva 2019/770, transposta para o direito nacional pelo Decreto-Lei n.º 84/2021, de 18 de outubro, e, por outro, na Diretiva 2019/2161, que alterou, entre outras diretivas, a Diretiva 2011/83/EU, sobre os direitos dos consumidores, no sentido de assegurar a sua coerência com o âmbito de aplicação da Diretiva 2019/770, e que obrigou à alteração de diversos diplomas em matéria de consumo, designadamente a Lei n.º 24/96, de 31 de julho, ou o Decreto-Lei n.º 24/2014, de 14 de fevereiro.

Apesar do expresso reconhecimento destes modelos de negócio no seio do direito do consumidor, a doutrina e a *soft law* têm identificado vários

pontos de conflito (e, para alguns, irresolúveis) com o Regulamento Geral sobre a Proteção de Dados, designadamente a dificuldade em encontrar um fundamento viável para assegurar a licitude do tratamento desses dados.

Não devendo o estudo de compatibilidade com o Regulamento Geral sobre a Proteção de Dados ser menosprezado, o presente trabalho procurará avaliar a eficácia com que o direito do consumidor tutela a vontade negocial do consumidor no momento da celebração desses contratos, e de que modo é que tal poderá contribuir para ultrapassar os potenciais óbices em sede de direito da proteção de dados pessoais, *maxime* através do preenchimento do fundamento de licitude da necessidade do tratamento de dados pessoais para a execução de um contrato em que o titular dos dados seja parte.

Palavras-chave: dados pessoais; contraprestação; consumidor; conteúdos digitais; serviços digitais.

Abstract: A significant number of business models operating in the digital economy entail the provision of personal data (and not any pecuniary asset) in exchange for the provision of digital content and services. These provisions, which the average consumer perceives as being "free of charge", have recently been recognized and framed in consumer protection law: on the one hand, in Directive 2019/770, transposed by Decree-Law no. 84/2021 of 18 October, and, on the other hand, in Directive 2019/2161, which amended, among other directives, Directive 2011/83/EU, on consumer rights, in order to ensure consistency with the scope of application of Directive 2019/770, and which led to the amendment of several laws on consumer matters, namely Law no. 24/96, of 31 July, and Decree-Law no. 24/2014, of 14 February.

Despite the express recognition of these business models within consumer protection law, doctrine and soft law have identified several points of conflict (and, for some, irresolvable) with the General Data Protection Regulation, namely the difficulty in finding a viable basis to ensure the lawfulness of the processing of such data.

As the study of compatibility with the General Data Protection Regulation should not be overlooked, this paper will seek to assess how consumer protection law supports the consumer's contractual will, and how it can contribute to overcome the potential data protection obstacles, notably by helping to meet the legal requirements of the lawful basis of the necessity for the performance of a contract to which the data subject is a party.

Keywords: personal data; counter-performance; consumer; defect; digital content; digital services.

cípio do pacta sunt servanda 3.2. A necessidade para a execução do contrato. Em especial, as Diretrizes 2/2019 do CEPD a) A amplitude do conceito indeterminado b) A avaliação da existência, em concreto, de uma "necessidade" c) As especificidades do tratamento dos dados pessoais para efeitos de publicidade comportamental em linha 3.3. A proposta de uma interpretação alternativa. Aplicação à Diretiva 2019/7704. A utilização de dados pessoais como contraprestação e o seu reflexo no equilíbrio contratual 4.1 Classificação do contrato a) Contrato sinalagmático ou não-sinalagmático b) Contrato gratuito ou oneroso 4.2 – A proteção da equivalência das prestações integradas no sinalagma a) A especial tutela do pacta sunt servanda num contrato sinalagmático b) O equilíbrio das (justas) prestações sinalagmáticas 5. O papel do Direito do Consumidor na (justa) formação do contrato e na composição do seu objeto 5.1 As obrigações pré-contratuais de informação, maxime sobre preços 5.2 – Os deveres de transparência impostos pelo Regime das Cláusulas Contratuais Gerais 6. Conclusões 7. Bibliografia

1. INTRODUÇÃO

Não cremos ser inovadora a conclusão de que o funcionamento da sociedade hodierna, em várias das suas vertentes – do profissional ao social e ao mais estrito pessoal – está largamente dependente de um determinado conjunto de serviços que o consumidor médio, mais ou menos instruído, perceciona como gratuitos, uma vez que o benefício dos mesmos não depende de qualquer contrapartida pecuniária. Arriscaríamos até dizer que a ausência de uma contrapartida pecuniária disfarça e omite, aos olhos do mesmo consumidor médio, a existência de uma verdadeira relação contratual com o fornecedor desses mesmos serviços.

Com efeito, a utilização *gratuita* de sítios na *internet* ou aplicações de *smartphone*, destinados a um largo conjunto de finalidades (*e.g.*, consumo e partilha de conteúdo audiovisual, serviços de comunicações interpessoais independentes de número, frequência e utilização de redes sociais, serviços de georreferenciação terrestre, entre outros), e disponibilizados por um vasto leque de empresas[1] ao abrigo de modelos contratuais atípicos (e, como veremos, sensíveis em vários domínios) e sem um enquadramento jurídico próprio, tem vindo a ganhar uma expressão que não pode ser ignorada pelos legisladores. De facto, em 2020, *gratuitamente* foi a palavra de ordem na transmissão de quase 30% dos s*oftwares antivirus*, *softwares* de pesquisa e serviços *cloud* comercializados, de 77% de serviços de *download* de con-

[1] Pela sua notoriedade e relevo no mercado, destacam-se as chamadas "*Big Four*", ou "GAFA" - Alphabet (antiga Google), Amazon, Meta (antiga Facebook) e Apple -, as quais, entre elas, dominam vários mercados de consumo. O impacto e peso económico destas *Big Four* é comumente ponderado num quinteto composto também pela Microsoft (*Big Five*), que, contudo, tem maior predominância no segmento empresarial e não consumista.

teúdos, como o *Spotify*, bem como de 50% dos videojogos, *e-books* e conteúdos televisivos[2].

Ora, perante este cenário, relembrar-nos-iam os economistas de que *não há almoços grátis*. É evidente - e de *La Palice* - que a prestação de serviços *gratuitos*[3] está associada a mecanismos de remuneração dos respetivos prestadores, aptos a cobrir os custos associados à sua prestação e a promover (e proteger) o investimento nas infraestruturas e recursos necessários.

O mercado oferece-nos múltiplos exemplos de modelos de negócio, desenhados para suportar os custos inerentes à disponibilização dos serviços *gratuitos*: a criação de modelos *premium* e a venda de anúncios publicitários sempre foram alternativas típicas para o financiamento da prestação desses serviços, aos quais se junta o fornecimento do (e pelo) utilizador dos serviços dos seus dados pessoais[4] em *troca* da utilização dos serviços *gratuitos* em causa[5].

Após a recolha desses dados, os mesmos serão tratados[6], gerando informação que será utilizada, a jusante, para servir diversas finalidades: não só para refinar as estratégias de venda de anúncios publicitários, mas para outros propósitos (do próprio profissional que recolhe os dados pessoais ou de terceiros compradores dessa informação), nomeadamente de avaliação

---

[2] Cf. Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer, "Data as Counter-Performance – Contract Law 2.0? An Introduction", *in* Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (*eds. lits.*), *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 10-11, e Irene Kull, "Withdrawal from the Consent to Process Personal Data Provided as Counter-Performance: Contractual Consequences"*, in Journal of the University of Latvia*, vol. 13 (2020), p. 35.

[3] É certo que estas empresas podem igualmente disponibilizar, onerosamente, certos serviços, designadamente versões *premium* dos serviços gratuitos, que, contra o pagamento de um determinado preço, oferecem determinadas vantagens e funcionalidades adicionais (e.g., remoção de anúncios publicitários, eliminação de *caps* de utilização, entre outros).

[4] O artigo 4.º, n.º 1 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (RGPD) define "dados pessoais" como "*informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular*".

[5] Cf. Madalena Narciso, "Dados Pessoais como Contraprestação em Contratos de Consumo – Breve Reflexão"*, in Anuário do NOVA Consumer Lab*, Ano 1, 2019 (janeiro 2020), p. 129.

[6] O artigo 4.º, n.º 1 do RGPD define "tratamento" como "*uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição*".

de risco (por exemplo, em seguradoras ou entidades bancárias), entre vários outros. Assim, a lógica destes modelos de negócio assenta na recolha de dados pessoais, no âmbito de relações de consumo, tendo em vista a sua ulterior utilização e tratamento para diversas finalidades capazes de remunerar o serviço prestado, como se de autêntico dinheiro se tratasse[7].

Num mundo em que os dados já absorveram o epíteto de, entre outras variantes, "*novo petróleo*"[8] e em que os *big data*[9] são o motor de uma parte considerável da economia digital, vê-se, assim, o enorme potencial de receita dos modelos de negócio que impliquem o fornecimento de dados pessoais, cujo valor económico, sendo elevado, é de difícil medição[10]. Por outro lado, é também inegável o contributo que este modo de pagamento tem para uma difusão equitativa e inclusiva dos serviços, uma vez que qualquer pessoa, independentemente do seu património, estará sempre em condições de pagar e beneficiar de um determinado conteúdo ou serviço[11].

Foi em reação ao incessante crescimento da expressão económica destes novos modelos de negócio (que, como vimos, suportam uma parte não menosprezável da economia), e ciente que estava da necessidade de proteger os utilizadores desses serviços *gratuitos*, que o legislador europeu, no contexto da sua Estratégia para o Mercado Único Digital na Europa[12], os reconheceu e enquadrou expressamente no direito do consumidor[13]. E fê-lo em dois eixos.

---

7 Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer, "Data as Counter-Performance – Contract Law 2.0? An Introduction", *ob. cit.*, p. 11, indicam mesmo que se os dados não são já hoje uma verdadeira moeda, tornar-se-ão uma moeda "de facto" no futuro.

8 De acordo com informação disponibilizada pela European Data Strategy no seu *website*, projeta-se que, em 2025, a riqueza gerada pela "economia dos dados" na União Europeia atinja €829 biliões, por contraposição aos €301 billion gerados em 2018: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en#projected-figures-2025 (24.05.2022).

9 Sobre o fenómeno dos *big data* e alguns dados ilustrativos da sua expressão na economia digital, *idem*, pp. 11-12, e ainda, para uma problematização sobre os cuidados e preocupações que o tratamento (automatizado) desses dados convoca, cf. Inês Silva Costa, "A proteção da pessoa na era dos *big data*: a opacidade do algoritmo e as decisões automatizadas", *in Revista Electrónica de Direito* (RED), publicação *online*, Vol. 24, n.º 1 (2021), pp. 33-82.

10 Sobre a medição do valor económico dos dados pessoais, cf. Philipp Hacker, "Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive", *in* Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (*eds. lits.*), *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 48 e ss.

11 Cf. Yoan Hermstrüwer, "Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data". *In Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (JIPITEC), Vol. 8, n.º 1 (2017), p. 9.

12 COM(2015) 192 final, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52015DC0192 (10.05.2022).

13 A temática do fornecimento de dados (pessoais ou não) como contraprestação extravasa, conceptual e teoricamente, a proteção do consumidor, apesar de ter sido este o palco da primeira intervenção específica nesta matéria por parte do legislador europeu. Martin Fries, "Data as Counter-Performance in B2B Contracts", *in Data as Counter-*

Por um lado, a Diretiva 2019/770[14], que procurou definir regras comuns em matéria de fornecimento de conteúdos[15] ou serviços digitais[16] a consumidores, de conformidade do fornecimento dos mesmos com o contrato, incluindo meios de ressarcimento em caso de falta de conformidade ou de não fornecimento, estendeu as suas normas aos contratos em que, a troco do fornecimento de conteúdos ou serviços digitais, o consumidor "*faculte ou se comprometa a facultar dados pessoais ao profissional, exceto se os dados pessoais facultados pelo consumidor forem exclusivamente tratados pelo profissional para fornecer os conteúdos ou serviços digitais em conformidade com a presente diretiva, ou para o profissional cumprir os requisitos legais a que está sujeito, não procedendo ao tratamento desses dados para quaisquer outros fins*" (artigo 3.º, n.º 1)[17]. Entre nós, a Diretiva 2019/770 foi transposta pelo Decreto-Lei n.º 84/2021, de 18 de outubro[18].

Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V, pp. 253-261, apresenta algumas notas sobre as preocupações que o fornecimento de dados como contraprestação levanta em sede de contratos B2B.

14 Diretiva (EU) 2019/770, do Parlamento Europeu e do Conselho, de 20 de maio de 2019, sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais, JO L 136, 22.5.2019, p. 1–27.

15 Para um estudo sobre o conceito de "conteúdo digital", à sua ligação a figuras paralelas e ao seu âmbito de proteção no quadro geral do direito do consumidor, cf. Hervé Jacquemin, "Contracting Around Privacy...", *ob. cit.*,, pp. 27–38.

16 Têm surgido iniciativas em que os dados pessoais servem como "remuneração", não só de serviços e conteúdos digitais, mas também em contratos sob bens e serviços "tradicionais": é o caso da *Shiru Cafe,* que oferece café a troco dos dados pessoais dos clientes (https://www.npr.org/sections/thesalt/2018/09/29/643386327/no-cash-needed-at-this-cafe-students--pay-the-tab-with-their-personal-data?t=1647456292117, acedido em 27.12.2021).

17 É de referir desde já que a Comissão Europeia, no contexto da preparação da Diretiva 2019/770, rejeitou expressamente a *gratuitidade* dos serviços prestados tendo o fornecimento de dados pessoais como contraprestação. Refere a Comissão Europeia que "[d]*ado o aumento do valor económico dos dados pessoais, esses serviços não podem ser considerados como «gratuitos»".* Cf. Proposta de Diretiva do Parlamento Europeu e do Conselho, que altera a Diretiva 93/13/CEE do Conselho, de 5 de abril de 1993, a Diretiva 98/6/CE do Parlamento Europeu e do Conselho, a Diretiva 2005/29/CE do Parlamento Europeu e do Conselho e a Diretiva 2011/83/UE do Parlamento Europeu e do Conselho, a fim de assegurar uma melhor aplicação e a modernização das normas da UE em matéria de defesa do consumidor, COM/2018/185 final – 2018/0090 (COD), p. 3.

18 O Decreto-Lei n.º 84/2021, de 18 de outubro, de resto, transpôs também a demais diretiva "gémea": a Diretiva (UE) 2019/771 relativa a certos aspetos dos contratos de compra e venda de bens, que altera o Regulamento (UE) 2017/2394 e a Diretiva 2009/22/CE e que revoga a Diretiva 1999/44/CE, JO L 136, 22.5.2019, p. 28–50.

Por outro lado, a Diretiva 2019/2161[19], que alterou, no que releva ao presente trabalho, a Diretiva 93/13/CEE[20], relativa às cláusulas abusivas nos contratos celebrados com consumidores, a Diretiva 2005/29/CE[21], que estabelece regras em matéria de práticas comerciais desleais, e a Diretiva 2011/83/EU[22], que estabelece os direitos dos consumidores, estendeu a aplicação desta última no sentido de assegurar a coerência com o âmbito de aplicação da Diretiva 2019/770[23]. A Diretiva 2019/2161 foi transposta para o direito interno em duas fases: *a primeira e a mais relevante para o objeto do presente estudo*, no final de 2021, através do Decreto-Lei n.º 109-G/2021, de 10 de dezembro, que alterou (no que aqui importa) a Lei n.º 24/96, de 31 de julho (Lei de Defesa do Consumidor), o Decreto-Lei n.º 446/85, de 25 de outubro (Regime das Cláusulas Contratuais Gerais), o Decreto-Lei n.º 57/2008, de 26 de marc o (Regime das Práticas Comerciais Desleais), e o Decreto-Lei n.º 24/2014, de 14 de fevereiro (Regime dos Contratos à Distância), diplomas estes que asseguravam a transposição das diretivas alteradas; *a segunda*, em março de 2023, através da Lei n.º 10/2023, de 3 de março, focada essencialmente em matéria sancionatória.

---

19 Diretiva (UE) 2019/2161, do Parlamento Europeu e do Conselho, de 27 de novembro de 2019, que altera a Diretiva 93/13/CEE do Conselho e as Diretivas 98/6/CE, 2005/29/CE e 2011/83/EU, do Parlamento Europeu e do Conselho, a fim de assegurar uma melhor aplicação e a modernização das regras da União em matéria de defesa dos consumidores, JO L 328, 18.12.2019, p. 7–28.

20 Diretiva 93/13/CEE do Conselho, de 5 de Abril de 1993, relativa às cláusulas abusivas nos contratos celebrados com os consumidores, JO L 95, 21.4.1993, p. 29–34.

21 Diretiva 2005/29/CE do Parlamento Europeu e do Conselho, de 11 de Maio de 2005, relativa às práticas comerciais desleais das empresas face aos consumidores no mercado interno e que altera a Diretiva 84/450/CEE do Conselho, as Diretivas 97/7/CE, 98/27/CE e 2002/65/CE e o Regulamento (CE) n.° 2006/2004, JO L 149, 11.6.2005, p. 22–39.

22 Diretiva (EU) 2011/83/UE do Parlamento Europeu e do Conselho de 25 de Outubro de 2011, relativa aos direitos dos consumidores, que altera a Diretiva 93/13/CEE do Conselho e a Diretiva 1999/44/CE do Parlamento Europeu e do Conselho e que revoga a Diretiva 85/577/CEE do Conselho e a Diretiva 97/7/CE do Parlamento Europeu e do Conselho, JO L 304, 22.11.2011, p. 64–88. É de salientar que a extensão do âmbito de aplicação da Diretiva (EU) 2011/83/UE operada pela Diretiva 2019/2161 se circunscreveu aos contratos de prestação de serviços digitais, uma vez que, nos termos do segundo o considerando 31 da Diretiva 2019/2161, a Diretiva 2011/83/EU "*já é aplicável aos contratos de fornecimento de conteúdos digitais que não sejam fornecidos num suporte material (a saber, o fornecimento de conteúdos digitais em linha), independentemente do facto de o consumidor pagar um determinado preço em dinheiro ou fornecer dados pessoais. Contudo, essa diretiva apenas se aplica aos contratos de serviços, incluindo os contratos de serviços digitais, ao abrigo dos quais o consumidor paga ou se compromete a pagar um preço. Por conseguinte, essa diretiva não é aplicável aos contratos de serviços digitais ao abrigo dos quais o consumidor fornece dados pessoais ao profissional sem pagar qualquer preço. Dadas as semelhanças entre estes serviços e a permutabilidade entre serviços digitais contra o pagamento de um preço e serviços digitais fornecidos em troca de dados pessoais, estes serviços deverão ser sujeitos às mesmas regras ao abrigo dessa diretiva*".

23 Cf. considerando 32 da Diretiva 2019/2161.

Ora, ao longo do presente trabalho, demonstraremos como a disciplina jurídica destas relações de consumo em que o consumidor fornece dados pessoais como contraprestação[24] em troco da prestação de conteúdos e serviços digitais aparenta ser, em alguns tópicos, conflituante com o RGPD[25]. Desde logo, levanta-se a necessidade de se encontrar um fundamento de licitude capaz de basear o tratamento dos dados pessoais fornecidos como contraprestação (artigo 6.º do RGPD), sendo que a prestação de consentimento, comumente apontado como o fundamento de licitude mais viável, suscita vários problemas de índole prática e jurídica que arriscam inviabilizá-lo.

Ao longo do presente texto, procuraremos avaliar a possibilidade de o tratamento dos dados pessoais fornecidos como contraprestação se basear no fundamento de licitude da necessidade para a execução de um contrato em que o titular dos dados seja parte, previsto no artigo 6.º, n.º 1, al. b) do RGPD. A aplicação desse fundamento de licitude obviaria a vários dos obstáculos colocados a este modelo de negócio por uma leitura isolada do RGPD, sem, ao mesmo tempo, comprometer a proteção concedida ao titular dos dados pessoais, que sempre seria convocado a assentir no tratamento dos seus dados pessoais (já não através de um consentimento autónomo, mas através da sua própria declaração negocial, devidamente informado e explicado).

Procuraremos, assim, contribuir para uma melhor compreensão dessa norma do RGPD, com apoio em princípios clássicos do direito dos contratos (de que o *pacta sunt servanda* e o equilíbrio prestacional figuram como bandeira) aplicáveis a relações jurídicas desta natureza, sem esquecer as normas específicas de proteção pré-contratual do consumidor aplicáveis, e que acima referimos, com as alterações introduzidas pelo Decreto-Lei n.º 109-G/2021, de 10 de dezembro.

É esse exercício que nos propomos realizar no presente trabalho.

---

[24] Como veremos, a adequação do conceito de "contraprestação", em si mesma, não é unânime. Porém, utilizá-lo-emos ao longo do nosso texto por facilidade de referência.

[25] De resto, e tal como apontam Sebastian Lohsse, Reiner Schulze, Dirk "taudenmayer, "Data as Counter-Performance – Contract Law 2.0? An Introduction", *ob. cit.*, p. 20, e Madalena Narciso, "Dados Pessoais como Contraprestação...", *ob. cit.*, p. 132, nota 11, também do ponto de vista dos direitos reais se justificaria analisar a questão, uma vez que não é pacífica a discussão sobre se os dados pessoais são objeto de direitos reais. Sobre a coisificação dos dados pessoais, cf. Patrícia Filipa Pereira Carneiro, "*Coisificação" dos dados pessoais no âmbito das relações contratuais*, FDUP, 2019 (dissertação de mestrado). Especificamente sobre a eventual qualificação dos dados pessoais como coisas, cf. Mafalda Miranda Barbosa, "Negócios onerosos e gratuitos: uma reflexão a propósito de novos fenómenos de gratuitidade"*, in Revista de Direito Comercial* (2020), pp. 1843 e ss. Em qualquer caso, considerações dessa natureza escapam ao âmbito e propósito do presente trabalho.

2. PROBLEMATIZAÇÃO CONCEPTUAL E ENQUADRAMENTO JURÍDICO

2.1. O FORNECIMENTO E TRATAMENTO DE DADOS COMO CONTRAPRESTAÇÃO NO QUADRO DA DIRETIVA 2019/770 E DO DECRETO-LEI N.º 84/2021, DE 18 DE OUTUBRO

Fruto da crescente expressão, na economia (digital) europeia, do fornecimento de conteúdos digitais, entrou em vigor, em 2019, a Diretiva 2019/770, sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais. Com um enquadramento meramente parcelar nas diretivas "gerais" de proteção do consumidor, entendeu o legislador europeu ser tempo de, em acréscimo ao regime geral vigente, conceder a esses contratos um enquadramento jurídico autónomo no seio do direito do consumidor, conferindo-lhes uma disciplina harmonizada e capaz de proteger os consumidores no âmbito destas relações. Esta Diretiva foi transposta para o ordenamento jurídico nacional, como já vimos, através do Decreto-Lei n.º 84/2021, de 18 de outubro.

Perante a crescente expressividade do fornecimento "gratuito" de conteúdos e serviços digitais no âmbito do Mercado Único Digital, o legislador tomou esta oportunidade para alargar o âmbito de aplicação da Diretiva 2019/770[26] aos contratos em que "(...) *o profissional forneça ou se comprometa a fornecer conteúdos ou serviços digitais ao consumidor e o consumidor faculte ou se comprometa a facultar dados pessoais ao profissional exceto se os dados pessoais facultados pelo consumidor forem exclusivamente tratados pelo profissional para fornecer os conteúdos ou serviços digitais em conformidade com a presente diretiva, ou para o profissional cumprir os requisitos legais a que está sujeito, não procedendo ao tratamento desses dados para quaisquer outros fins*"[27]. Assim, indo mais longe do que a

---

[26] Analisando em detalhe o âmbito de aplicação da Diretiva 2019/770, cf. Karin Sein, Gerald Spindler, "The new Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1", *in European Review of Contract Law*, Vol. 15, n.º 3 (2019), pp. 265 e ss.

[27] Cf. artigo 3.º, n.º 1, *in fine*, e considerando 24 da Diretiva 2019/770, e artigo 3.º, n.º 3, al. b) do Decreto-Lei n.º 84/2021, de 18 de outubro. Tal com aponta Jorge Morais Carvalho, *Compra e Venda e Fornecimento de Conteúdos e Serviços Digitais – Anotação ao Decreto-Lei n.º 84/2021, de 18 de outubro*, Coimbra, Almedina, 2022, p. 28, "*apenas devem ser considerados como contraprestação os dados pessoais tratados para fim que não seja estritamente necessário para o cumprimento do contrato ou de um dever legal*". Assim, parece decorrer da parte final deste preceito que a disciplina do Decreto-Lei n.º 84/2021, de 18 de outubro (e da Diretiva 2019/770) não deverá aplicar-se aos casos em que o profissional trate dados pessoais, não com finalidades de contraprestação, mas enquanto necessidade (acrescentamos, *operacional*, por razões que adiante aprofundaremos) para a correta prestação desses fornecimentos ou para o cumprimento de uma obrigação legal (pensemos, *e.g.*, e respetivamente, no tratamento do nome para efeitos de criação de um endereço de e-mail e na divulgação de dados pessoais no âmbito de obrigações impostas

consagração de uma disciplina jurídica própria para estes contratos de consumo, a Diretiva 2019/770 reconhece, legitima e submete ao mesmo regime os modelos de negócio assentes no "pagamento" através do fornecimento de dados pessoais, de um modo que, conforme *infra* aludiremos, não permitiu dissipar algumas das preocupações que já durante o procedimento legislativo foram antecipadas.

Esse esforço das instituições europeias, na nossa ótica, pecou por defeito. Por um lado, o legislador relegou para o RGPD todo o enquadramento dessas operações de tratamento de dados pessoais[28], não tendo logrado harmonizar a aplicação dos dois diplomas (a qual, como veremos, já durante o procedimento legislativo havia sido demonstrada ser conflituante). Por outro lado, o legislador europeu delegou no direito nacional todas as considerações de direito geral dos contratos[29]. A respeito deste último, a Diretiva 2019/770 demarcou-se deliberadamente de tomar posição quanto à qualificação jurídica dos contratos sob a sua regulação, à luz dos recortes e figuras contratuais típicas tradicionais (*e.g.*, enquanto contratos de compra e venda, contratos de prestação de serviços, ou, em certos casos, contratos de aluguer, entre outros...)[30]. Esta subsunção caberá ao direito interno aplicável[31], cabendo-lhe ainda toda a disciplina de responsabilidade contratual que não esteja coberta pela Diretiva 2019/770, designadamente

por legislação sobre combate ao branqueamento de capitais). Ora, apesar da proximidade da letra da referida norma com aquela impressa no artigo 6.º, n.º 1, als. b) e c) do RGPD, não deve interpretar-se aquela exclusão do âmbito de aplicação da Decreto-Lei n.º 84/2021, de 18 de outubro, como indexada à operação de um dos referidos fundamentos de licitude. Ao invés, e especificamente no que concerne à exclusão do âmbito de aplicação desses diplomas em virtude do tratamento de dados pessoais para fins de execução do contrato, aquilo que, na nossa opinião, o legislador procurou garantir foi que o tratamento de dados pessoais exclusivamente para assegurar a execução operacional do contrato não determinaria, de mote próprio, a sujeição ao seu regime – questão a que o fundamento de licitude utilizado (que, em tese, poderia ser ainda um dos outros do elenco do artigo 6.º, n.º 1, do RGPD, *maxime* o consentimento do titular dos dados) é alheio. Assim, cremos que não se encontram necessariamente excluídos do âmbito de aplicação Decreto-Lei n.º 84/2021, de 18 de outubro e da Diretiva 2019/770 os contratos em que o profissional, com base no fundamento de licitude do artigo 6.º, n.º 1, als. b) do RGPD, trate dados pessoais para efeitos de assegurar a exequibilidade *económica* do contrato, no sentido que procuraremos defender neste texto. Sobre o mesmo assunto, cf. Furkan Güven Taştan, *The (im)possibility of personal data as an object of contracts: An analysis of the GDPR and the Digital Content Directive*, Tilburg, Universidade de Tilburg, julho 2021, pp. 41-42 e 46-48.

28 Cf. artigo 3.º, n.º 8 da Diretiva 2019/770 e artigo 52.º, n.º 2 do Decreto-Lei n.º 84/2021, de 18 de outubro.

29 Cf. artigo 3.º, n.º 10 da Diretiva 2019/770.

30 A escolha do legislador por não tomar posição quanto à qualificação jurídica dos negócios em que dados pessoais sejam fornecidos como contraprestação justificar-se-á pelo receio do legislador europeu de que a classificação que cristalizasse fosse ultrapassada pela dinâmica comercial e pela inovação tecnológica. Cf. Karin Sein, Gerald Spindler, "The new Directive…", *ob. cit.*, p. 260.

31 Cf. considerando 12 da Diretiva 2019/770.

num cenário de incumprimento por parte do consumidor. Por outro lado, ainda, já avisado da falta de clareza destes modelos de negócio aos olhos do consumidor, o legislador não talhou deveres de informação e esclarecimento contratual específicos para este âmbito[32].

Estas omissões, no nosso entender, geram, por um lado, múltiplas dúvidas na tarefa de conciliação da utilização de dados como contraprestação em contratos com o regime do RGPD[33]; e, por outro, uma necessidade de refletir sobre se as atuais regras aplicáveis à formação destes contratos, e à definição do seu conteúdo, oferecem as garantias necessárias à proteção do consumidor. Uma resposta negativa a esta última questão poderá determinar a própria inviabilidade contratual deste modelo de negócio; uma resposta positiva poderá, ainda, permitir ultrapassar os óbices tradicionalmente apontados em matéria de proteção de dados pessoais.

O desafio central da questão, cremos, prende-se com a própria ciência do consumidor quanto aos termos essenciais da relação contratual, a qual sustentará não só o *esclarecimento*[34] *do consentimento* do titular dos da-

---

[32] A este propósito, salientamos que Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer, "*Data as Counter-Performance – Contract Law 2.0? An Introduction*", *ob. cit.*, p. 18, chamam a atenção para o facto de que os consumidores poderão nem sequer estar cientes de que estes "serviços gratuitos" estão contratualmente cobertos. Axel Metzger, "A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services", in Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (*eds. lits.)*, *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 30-31, aborda o modelo de formação destes contratos, pegando em alguns exemplos concretos (*Facebook*, *WhatsApp*, *Spotify* e *Google*), que interpreta como constituindo propostas contratuais.

[33] Por exemplo, a doutrina discute qual o impacto, ao nível contratual e da sua sujeição à Diretiva 2019/770 e ao Decreto-Lei n.º 84/2021, de 18 de outubro, de um tratamento ilícito dos dados pessoais fornecidos como contraprestação, havendo quem defenda que este implica a invalidade desses contratos e, por isso, a sua exclusão do âmbito de aplicação dos referidos normativos. Cf. Matilde Lopes Bettencourt, "A proteção do consumidor em contratos digitais: análise dos contratos celebrados com dados pessoais como contraprestação", *in Anuário do NOVA Consumer Lab*, Ano 3 (2021), pp. 439 e ss.

[34] Esclarecimento este inerente, por exemplo, ao (des)conhecimento, por parte do respetivo titular, sobre o valor dos seus dados pessoais e sobre a riqueza que os mesmos são suscetíveis de gerar, ou à circunstância de que a recusa do consentimento implica a negação do fornecimento do conteúdo ou serviço digital, enquanto efeito negativo suscetível de inquinar a liberdade do consentimento. De resto, para além da problemática do esclarecimento do titular dos dados, a liberdade do consentimento revela-se difícil de assegurar, atento o artigo 7.º, n.º 4 do RGPD, conforme abaixo abordamos.

dos pessoais[35] - que tem vindo a ser apontado[36] como o único fundamento capaz de sustentar a licitude do tratamento de dados pessoais fornecidos como contraprestação -, como também ao *esclarecimento da própria declaração negocial* emitida pelo consumidor, e que concorrerá, ele próprio, para sustentabilidade jurídica do contrato.

Ora, pode equacionar-se se uma correta formação do contrato à luz das normas legais aplicáveis abrirá caminho à defesa de que os dados pessoais fornecidos como contraprestação sejam tratados sem a necessidade de obtenção do consentimento. Isto porque o tratamento desses dados pessoais, de um ponto de vista jurídico-económico, poderá entender-se como necessário à execução do próprio contrato de fornecimento de conteúdos ou serviços digitais no âmbito do qual foram fornecidos[37], porquanto só com o seu tratamento, nos precisos termos estabelecidos contratualmente, o profissional poderia assegurar o equilíbrio económico do sinalagma. Esta solução, sendo viável, poderia dissipar (alguma d)a nebulosa em torno da compatibilidade entre estes negócios e o RGPD, sem prejudicar a posição

---

35 Cf. artigo 6.º, n.º 1, al. a) e artigo 7.º, n.º 4 do RGPD, norma esta que, de resto, determina a falta de liberdade do consentimento quando, sem ele, o prestador se recuse a prestar os serviços ou a fornecer os bens ou conteúdos digitais. Não se menospreza, por outro lado, a discussão de fundo sobre se, do próprio ponto de vista conceptual e atendendo ao estatuto de direito fundamental concedido à proteção de dados, é admissível a *monetização* dos dados pessoais. A este respeito, cf. a tímida (e, a nosso ver, problemática) alusão da Diretiva 2019/770, no seu considerando 24, que, reconhecendo embora a natureza de direito fundamental à proteção de dados pessoais e rejeitando a qualificação dos dados pessoais como "*commodity*" (ou "*produto de base*"), não logrou enquadrar e compatibilizar juridicamente o pagamento com dados pessoais com os inerentes valores e princípios. Com efeito, este texto operou meramente um recorte pela negativa (isto é, os dados pessoais *não* podem ser considerados um produto base e a Diretiva 2019/770 *não* prejudica a natureza de direito fundamental da proteção de dados pessoais), ao invés de introduzir uma definição positiva da fronteira de todos os princípios e interesses em jogo. Numa palavra, se o legislador optou por incluir essa referência na letra dos seus considerandos, não se escusou de desenhar a Diretiva 2019/770 independentemente dela. Embora aludamos à discussão neste trabalho, não nos centraremos nela, porque (e antecipando já) cremos que o direito à proteção de dados, enquanto direito de personalidade (artigo 70.º do Código Civil), não impede a exploração patrimonial desses mesmos dados pessoais, a qual, aliás, não é novidade (pense-se, *e.g.*, na cedência de direitos de imagem). Acrescentaríamos, até, que o segundo é uma decorrência do primeiro. Neste sentido, cf. Madalena Narciso, "Dados Pessoais como Contraprestação...", *ob. cit.*, pp. 134-135.

36 A posição de que o consentimento do titular dos dados constitui o único fundamento de licitude viável para sustentar o tratamento dos dados pessoais fornecidos como contraprestação surge influenciada, parece-nos, pela circunstância de a Diretiva 2019/770, a nosso ver erradamente, ter feito expressa referência ao consentimento (sem determinar a sua necessidade, mas apenas numa lógica de eventual necessidade) nos seus considerandos 38 e 40 - logo após enunciar que o RGPD mantinha o seu natural domínio de aplicação em matéria de proteção de dados pessoais. Cf., por exemplo, Yoan Hermstrüwer, "*Contracting Around Privacy…*", *ob. cit.*, p. 10.

37 Cf. artigo 6.º, n.º 1, al. b) do RGPD.

jurídica do consumidor, enquanto titular de dados pessoais, que manteria o controlo último sobre os seus dados, ao permitir evitar (e tornar redundante) a necessidade da recolha do consentimento do respetivo titular.

2.2. A DIFÍCIL COMPATIBILIZAÇÃO COM O RGPD

a) O papel e a inserção do RGPD na ordem jurídica (breve referência)

Os dados pessoais – e, de um modo geral, o bem jurídico da privacidade – gozam, no ordenamento jurídico da União Europeia, de uma elevada proteção, sendo o RGPD o seu maior sustentáculo[38]. A sua interpretação e aplicação é suportada, não só pela jurisprudência do Tribunal de Justiça da União Europeia, mas também por um vasto conjunto de *soft law* interpretativa (designadamente opiniões e orientações) emitida por entidades como a Autoridade Europeia para a Proteção de Dados (doravante, AEPD), o Comité Europeu de Proteção de Dados (doravante, CEPD), bem como pelas autoridades nacionais de proteção de dados, entre nós a Comissão Nacional de Proteção de Dados (doravante, CNPD).

A crescente proteção jurídica conferida à privacidade e à proteção de dados pessoais encontra o seu apoio no direito originário da União Europeia, designadamente no artigo 16.º, n.º 1, do Tratado Sobre o Funcionamento da União Europeia, que consagra que "*todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito*". Esta proteção ganhou ainda o estatuto de direito fundamental, concretamente no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia[39] - estatuto esse que, de resto, a Diretiva 2019/770 reconhece expressamente[40]. Assim, em matéria de proteção de dados pessoais, o RGPD assume o papel de "voz" do artigo 8.º da Carta dos Direitos Fundamentais da União Europeia e do artigo 16.º do Tratado Sobre o Funcionamento da União Europeia: é o diploma que estabelece as regras e os princípios basilares por que se rege o tratamento de dados pessoais em toda a atividade económica. Este estatuto é, aliás, reconhecido pela Diretiva 2019/770, que se afasta expressamente, como já vimos, através do seu artigo 3.º, n.º 8, de qualquer confronto com o RGPD (e com a Diretiva ePrivacy[41]).

---

[38] Ao nível do direito português, sendo certo o seu carácter pouco inovador para o que aqui releva, atenta a aplicabilidade direta do RGPD, importa mapear a Lei n.º 58/2019, de 8 de agosto, veio assegurar a execução desse regulamento na ordem jurídica nacional.

[39] Carta dos Direitos Fundamentais da União Europeia, JO C 326, 26.10.2012, pp. 391–407.

[40] Cf. considerando 24 da Diretiva 2019/770, já acima referido.

[41] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas JO L 201, 31.7.2002, p. 37–47.

O RGPD desenvolve e implementa as bases para a efetiva vigência desse direito fundamental, conforme referido no seu considerando 1[42] e reconhecido pela AEPD, na sua Opinião 4/2017[43]. Em poucas palavras — que sempre pecarão por defeito atenta a complexidade da questão e, para os propósitos deste trabalho, apenas entendermos necessário o enquadramento fundamental —, a proteção conferida pelo RGPD assenta, sobretudo, nos princípios do lícito, leal e transparente tratamento de dados pessoais, o qual deve abranger tão-só os dados pessoais estritamente necessários e ser limitado às finalidades para as quais são recolhidos (artigo 5.º, n.º 1, als. a) a c), do RGPD).

Esses princípios gerais materializam-se, fundamentalmente, de três modos. *Em primeiro lugar*, através da imposição de obrigações de informação ao titular dos dados pessoais quanto aos termos em que os seus dados serão tratados (artigos 13.º[44] e 14.º do RGPD). *Em segundo lugar*, no reconhecimento de direitos aos titulares sobre os seus dados pessoais, dando-lhes a possibilidade de, por exemplo, exigir a retificação dos seus dados pessoais, o seu apagamento, a limitação do tratamento e, em certos casos, o direito de se opor ao tratamento (respetivamente, artigos 16.º, 17.º, 18.º e 21.º do RGPD). *Em terceiro lugar*, mas não menos importante, na necessidade de basear o tratamento num dos fundamentos de licitude tipificados no artigo 6.º, n.º 1, do RGPD. É este, portanto, o panorama geral de limitações que um profissional deverá assegurar para que, licitamente, trate os dados pessoais que lhe sejam fornecidos a título de contraprestação.

b) O consentimento como fundamento de licitude

Em concreto, porém, e conforme já antecipado, a aplicação destas constelações normativas aos contratos em tese revela-se complexa, tendo vindo

---

42 "*A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.*"

43 Cf. European Data Protection Supervisor, *Opinion 4/2017, on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, p. 8. Esta opinião foi emitida a propósito da discussão, no Conselho, da Proposta de Diretiva COM/2015/0634 final, do Parlamento Europeu e do Conselho, sobre certos aspetos relativos aos contratos de fornecimento de conteúdos digitais, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A52015PC0634, e que viria a originar a Diretiva 2019/770 (doravante, Proposta de Diretiva 2019/770). Note-se, a título de detalhe, que, ao contrário da Diretiva 2019/770, a Proposta de Diretiva 2019/770 não abrangia a prestação de serviços digitais no seu âmbito de aplicação.

44 Para os casos que aqui apreciamos, é de destacar a obrigação que impende sobre o responsável pelo tratamento de informar o titular dos dados de que "*a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados*" (artigo 13.º, n.º 2, al. e), do RGPD).

a ser particularmente discutido quais os fundamentos de licitude mais adequados. Como tais, apontam-se, de um ponto de vista teórico, o consentimento[45] do titular dos dados, a necessidade para execução do contrato de fornecimento de conteúdos e serviços digitais e a existência de interesses legítimos do responsável pelo tratamento (respetivamente, alíneas a), b) e f) do n.º 1 do artigo 6.º do RGPD).

Apesar de serem equacionáveis três fundamentos de licitude, a discussão tende a focar-se no *consentimento do titular dos dados*, não sendo as demais alternativas, a nosso ver, suficientemente exploradas[46]. Não cremos que esta monopolização se justifique. Se, por um lado, se compreende que a recolha do consentimento é o fundamento de licitude que confere, em geral, um maior controlo ao titular dos dados sobre o tratamento dos seus dados pessoais, por outro cremos não ser de ignorar que levanta inúmeros e desnecessários problemas prático-jurídicos, com prejuízos para o livre funcionamento do mercado, constituindo um dos polos de conflito entre estes modelos de negócio e o RGPD[47]. De resto, na sua essência está a proteção de um interesse – a liberdade do titular dos dados para permitir o tratamento dos seus dados pessoais – que poderá ser protegido, com a mesma eficácia, através de uma declaração negocial, enquanto ato (único) de expressão da sua vontade.

Um dos problemas atinentes a este fundamento de licitude prende-se com a liberdade do consentimento[48]. Com efeito, o artigo 7.º, n.º 4, do RGPD

---

[45] O artigo 4.º, n.º 11 do RGPD define o consentimento do titular dos dados como "*uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*". Estes requisitos são densificados em *soft law*, no considerando 43**,** bem como noutras disposições do RGPD, sobretudo o seu artigo 7.º, que imputa ao responsável pelo tratamento o ónus da prova da validade desse consentimento.

[46] Parece ser esta a posição de Madalena Narciso, "Dados Pessoais como Contraprestação...", *ob. cit.*, pp. 145 e ss., Axel Metzger, "Data as Counter-Performance: What Rights and Duties do Parties Have?", *in Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (JIPITEC), Vol. 8, n.º 1 (2017), p. 5, Irene Kull, "Withdrawal from the Consent…", *ob. cit.*, p. 42 e Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer, "*Data as Counter-Performance – Contract Law 2.0? An Introduction*", *ob. cit.*, pp. 19-20.

[47] Conforme aponta Giuseppe Versaci, "Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection", *in European Review of Contract Law*, Vol. 4, n.º 4 (2018), pp. 378 e ss. É de salientar, em todo o caso, e porque especialmente relevante, que a invalidade do consentimento para o tratamento de dados pessoais não subtrairia automaticamente o contrato do âmbito de aplicação da Diretiva 2019/770, o que, paradoxalmente, apenas teria como efeito a diminuição da proteção do consumidor-titular dos dados. Cf. Axel Metzger, "A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services", *ob. cit.*, pp. 33-34. Sobre mesmo assunto, e também sobre o efeito do tratamento ilícito de dados pessoais na validade do contrato, cf. Philipp Hacker, "Regulating the Economic Impact of Data as Counter-Performance...", *ob. cit.*, pp. 56 e ss.

[48] Sobre a dificuldade em obter um consentimento livre no contexto de *big data*, cf. Inês Silva Costa, "A proteção da pessoa na era dos *big data*...", *ob. cit.,* pp. 51-53.

faz relevar, como circunstância necessária à avaliação da liberdade do consentimento, a hipótese da recusa da prestação do serviço caso o consentimento não seja prestado, ponto que, como intuitivamente se compreende, assume uma grande relevância no contexto da celebração de contratos bilaterais, como aqueles em análise[49]. Assim, pese embora esta norma não condene necessariamente o consentimento à sua falta de liberdade[50], atribui-lhe incerteza jurídica[51] e, se se concluir, *in casu*, pela ilicitude daquele ato, já os dados pessoais terão sido tratados ilicitamente, com prejuízos para a esfera jurídica do respetivo titular.

Por outro lado, seria de duvidar, em certos casos, do esclarecimento do consentimento, uma vez que, e tal como aponta o CEPD nas suas Diretrizes 2/2019, a coexistência de vários fundamentos de licitude como base para diferentes operações de tratamento de dados pessoais envolvidas na execução de um mesmo contrato[52] (além do ato de manifestação da vontade negocial propriamente dito) acarretaria o risco da falta de discernimento do titular dos dados, uma vez que "*consoante as circunstâncias, os titulares dos dados podem ter a impressão errada de que estão a dar o seu consentimento nos termos do artigo 6.º, n.º 1, alínea a), ao assinarem um contrato ou ao aceitarem as condições de serviço. Ao mesmo tempo, um responsável pelo tratamento*

---

[49] Seguindo o raciocínio de Matilde Lopes Bettencourt, "A proteção do consumidor...", *ob. cit.*, p. 441, nestes casos em que o sinalagma que se forma une o fornecimento do conteúdo ou serviço digital em causa ao fornecimento dos dados pessoais propriamente ditos, o consentimento para o seu tratamento assume-se como um requisito (jurídico) prévio da utilidade (jurídico-económica) desses dados pessoais. Assim, pretendendo um profissional apoiar no consentimento o tratamento dos dados pessoais que lhe hajam sido fornecidos como contraprestação, e não podendo o mesmo obter licitamente qualquer vantagem desses dados sem a obtenção desse consentimento, parece-nos razoável que a celebração do negócio fique condicionada à prestação desse consentimento.

[50] Concordamos, assim, com Axel Metzger, "Data as Counter-Performance…", p. 5. Porém, parece ser mais rígida a posição do European Data Protection Supervisor, *Opinion 4/2017…, ob. cit.,* §55, p. 15, ao referir que o RGPD "*creates a presumption that the consent is not freely given when it is a conditional to receive the provision of a service "despite such consent not being necessary for such performance*".

[51] Para solucionar esta aparente impossível liberdade do consentimento, tem sido proposta a disponibilização constante de um modelo alternativo para aceder aos conteúdos e serviços digitais através do pagamento de dinheiro. Reconhecendo a sua bondade, duvidamos da viabilidade plena desta solução, uma vez que, em certos casos, o titular dos dados pode não dispor de um poder de compra que lhe confira, efetivamente, uma escolha livre. De resto, essa hipótese não solucionaria a possível ilicitude do consentimento pela falta de esclarecimento do titular dos dados. Neste sentido, cf. Yoan Hermstrüwer, "*Contracting Around Privacy…*", ob. cit., p. 17 e ss.

[52] Pense-se, por exemplo, num contrato para abertura de conta numa rede social, em que o nome e a idade do titular dos dados serviriam propósitos de contraprestação (a serem tratados ao abrigo do artigo 6.º, n.º 1, al. a) do RGPD), de criação do próprio perfil público na rede social (uma necessidade operacional de execução do contrato, apoiada no artigo 6.º, n.º 1, al. b) do RGPD), podendo ainda ser tratados para efeitos de cumprimento de obrigações legais, ao abrigo do artigo 6.º, n.º 1, al. c) do RGPD.

pode presumir erradamente que a assinatura de um contrato corresponde a um consentimento na aceção do artigo 6.º, n.º 1, alínea a)" [53].

Por fim, sempre se colocaria o tema clássico, e já acima referido, sobre quais as consequências contratuais da retirada do consentimento[54].

Assim, testemunhando as dificuldades inerentes ao recurso à recolha do consentimento do titular dos dados, e atento o facto de não vislumbrarmos, na situação em análise no presente trabalho, interesses que só assim possam ser defendidos (como demonstraremos), cremos justificar-se uma reflexão sobre a viabilidade do recurso à necessidade para a execução de um contrato em que o titular dos dados seja parte (artigo 6.º, n.º 1, al. b) do RGPD), enquanto base para a licitude do tratamento de dados fornecidos como contraprestação.

c) Os dados pessoais enquanto commodity

É longa e complexa a discussão em torno da própria compatibilidade do conceito de utilização de dados pessoais como contraprestação com o RGPD e com a natureza jusfundamental[55] desse direito. Esta discussão foi particularmente expressiva no seio da discussão da Proposta de Diretiva 2019/770, a qual previa expressa e literalmente o fornecimento de dados como um ato de *contraprestação*[56] pela prestação de certos serviços ou pela disponibilização de certos conteúdos digitais, o que gerou uma forte oposição por parte da AEPD[57]. Com efeito, e segundo esta entidade, a natureza jusfundamental

---

[53] Cf. Comité Europeu de Proteção de Dados, *Diretrizes 2/2019 sobre o tratamento de dados pessoais ao abrigo do artigo 6.º, n.º 1, alínea b), do RGPD no contexto da prestação de serviços em linha aos titulares dos dados*, §20, p. 8.

[54] Para uma análise mais desenvolvida sobre os efeitos contratuais da retirada do consentimento, cf. Irene Kull, "Withdrawal from the Consent…", pp. 43 e ss, e, Martin Schmidt-Kessel, "Right to Withdrawn Consent to Data Processing – The Effect on the Contract", *in Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*, pp. 129-146. Sobre a possibilidade de o prestador de serviços "gratuitos" poder vir a ser indemnizado pelos danos causados pela retirada do consentimento, e sobre a hipótese de o mesmo continuar o tratamento dos dados pessoais do titular com base no interesse legítimo, e apesar de não nos revermos em vários pontos levantados, cf. Patrícia Filipa Pereira Carneiro, "*Coisificação" dos dados pessoais...", ob. cit.,* pp. 17 e ss.

[55] Cf. artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia.

[56] Cf., por exemplo, os Considerandos 13 e 37 e artigo 3.º, n.º 1 da Proposta de Diretiva 2019/770.

[57] Cf. European Data Protection Supervisor, *Opinion 4/2017..., ob. cit.* No seguimento da oposição oferecida pelo EDPS, esta terminologia viria a ser abandonada na Diretiva 2019/770, que, pese embora sem recuar na inserção destas modalidades contratuais no seu âmbito de aplicação, viria a abordar os mesmos casos como aqueles em que "*o consumidor faculte ou se comprometa a facultar dados pessoais ao profissional, exceto se os dados pessoais facultados pelo consumidor forem exclusivamente tratados pelo profissional para fornecer os conteúdos ou serviços digitais em conformidade com a presente diretiva, ou para o profissional cumprir os requisitos legais a que está sujeito, não procedendo ao tratamento desses dados para quaisquer outros fins*" (artigo 3.º, n.º 1,

do direito à proteção de dados poderá constituir um obstáculo à viabilidade deste modelo de negócio, uma vez que os seus atores sempre deverão atentar a que se trata de um direito indisponível[58], sendo por isso sensível a sua introdução no comércio, enquanto objeto de contratos sinalagmáticos.

Já em 2016, na sua Opinião 8/2016[59], a AEPD alertara para que, no espaço da União Europeia, a "informação pessoal" não pode ser entendida como um mero bem económico (*mere economic asset*), uma vez que está em causa o direito (fundamental) à proteção de dados pessoais, protegido pela Carta dos Direitos Fundamentais da União Europeia, e entendido pelo Tribunal Europeu dos Direitos do Homem como fundamental para garantia do efetivo gozo e exercício dos direitos ao respeito pela vida privada e da liberdade de expressão e associação[60].

A mesma entidade viria então a repescar esta argumentação na sua Opinião 4/2017 e a sustentar nela uma das principais críticas à Proposta de Diretiva 2019/770: a abertura expressa, que demonstrava, ao "pagamento" através do fornecimento de dados pessoais[61]. Com uma argumentação que nos parece fundamentalista, a AEPD criticou esta abordagem, tendo sido lapidar ao referir que os dados pessoais não são um *commodity*, não podendo, por isso, ser comparados a dinheiro[62], nem, em decorrência, servir como modalidade de *pagamento* como se do pagamento de um *preço* se tratasse. No entendimento da AEPD, os dados pessoais, porque protegidos por um direito

in fine, da Diretiva 2019/770, e artigo 3.º, n.º 3, al. b) do Decreto-Lei n.º 84/2021, de 18 de outubro). Cf. Jorge Morais Carvalho, *Compra e Venda e Fornecimento de Conteúdos e Serviços Digitais...*, *ob. cit.*, p. 28

58 Cf. Madalena Narciso, "Dados Pessoais Como Contraprestação...", *ob. cit.,* p. 133.

59 Cf. European Data Protection Supervisor, "Opinion 8/2016 - EDPS Opinion on coherent enforcement of fundamental rights in the age of big data*".*

60 Cf. *idem,* p. 7.

61 A mesma ideia viria ainda a ser reforçada pelo Comité Europeu de Proteção de Dados, que, a propósito do tratamento de dados pessoais para efeitos de publicidade comportamental, sublinhou que "*a proteção de dados é um direito fundamental garantido pelo artigo 8.º da Carta dos Direitos Fundamentais, e tendo em conta que um dos principais objetivos do RGPD consiste em proporcionar aos titulares dos dados o controlo das informações que lhes dizem respeito, os dados pessoais não podem ser considerados uma mercadoria comercializável. Mesmo que o titular dos dados possa concordar com o tratamento de dados pessoais, não pode dispor dos seus direitos fundamentais através deste acordo*". Cf. Comité Europeu de Proteção de Dados, *Diretrizes 2/2019..., ob. cit.*, §55, p. 16.

62 Esta incomparabilidade entre o fornecimento de dados pessoais e o dinheiro revela-se, por exemplo, pelo facto de que o consumidor não consegue medir a riqueza que gerará em benefício do profissional, ao contrário do que sucede perante uma contraprestação monetária; por outro lado, a possibilidade de os mesmos dados pessoais poderem ser fornecidos em múltiplas ocasiões, o que não sucede com o dinheiro, que não é "multiplicável"; ou também o regime da restituição, quando o profissional a tal esteja obrigado, que se afigura de difícil execução em caso de fornecimento de dados pessoais como contraprestação. Para maior desenvolvimento, cf. European Data Protection Supervisor, *Opinion 4/2017… ob. cit.,* §24-28, pp. 9-10, e Matilde Lopes Bettencourt, "A proteção do consumidor...", *ob. cit.*, p. 429.

fundamental, não são *comercializáveis*. A AEPD vai ainda mais longe neste raciocínio, exemplificando que a existência fáctica de mercados comerciais sobre órgãos humanos não implica que o legislador deva reconhecê-los ou validá-los, lógica que estende aos dados pessoais[63]. Aliás, a AEPD refere mesmo que "*one cannot monetise and subject a fundamental right to a simple commercial transaction, even if it is the individual concerned by the data who is a party to the transaction*". Nessa medida, defende, o legislador não poderia desconsiderar a específica natureza e regime jurídico dos dados pessoais[64] no exercício de regulação da utilização de dados pessoais como contraprestação contratual.

Em reação à posição da AEPD, o legislador europeu procurou, na Diretiva 2019/770, mitigar os riscos de incompatibilidade do seu regime com a natureza e legislação sobre proteção de dados. Com efeito, no considerando 24 da Diretiva 2019/770, o legislador reconheceu expressamente a natureza de direito fundamental da proteção de dados pessoais e rejeitou a sua qualificação como uma "*commodity*" (ou "*produto de base*", na versão portuguesa). Todavia, trata-se de um exercício de compatibilização, a nosso ver, tímido e sem impacto jurídico, uma vez que o diploma continuou a abranger a mesma realidade e, grosso modo, em termos idênticos (e que viriam a ser transpostos, a nosso ver adequadamente, para o Decreto-Lei n.º 84/2021, de 18 de outubro, e onde, de resto, o legislador nacional não toma posição sobre a temática em apreço[65]). Assim, esta ressalva não parece constituir mais do que uma mera tomada de posição política quanto ao estatuto dos dados pessoais no contexto da economia dos contratos "gratuitos".

Apesar das preocupações levantadas pela AEPD, não cremos existir um obstáculo à introdução de dados pessoais no objeto contratual como contraprestação. Em primeiro lugar, revela-se exagerada a confusão entre a atribuição do acesso a dados pessoais a terceiros, juridicamente enquadrada pelo RGPD, a alienação desses mesmos dados pessoais e, sobretudo, a renúncia ao direito fundamental à sua proteção. É no plano da primeira destas três hipóteses que o fornecimento de dados pessoais como contraprestação (e respetivo tratamento) se insere, não implicando as demais. Se as operações de tratamento respeitarem os limites impostos pelo RGPD, o titular mantém o

---

63 Cf. European Data Protection Supervisor, *Opinion 4/2017…*, *ob. cit.,* §14-17, p. 7.

64 Cf. Irene Kull, "Withdrawal from the Consent…", *op. cit.,* p. 36.

65 A CNPD, nos pareceres que emitiu no contexto dos procedimentos legislativos do Decreto-Lei n.º 84/2021, de 18 de outubro, e do Decreto-Lei n.º 109-G/2021, de 10 de dezembro, tomou uma posição que nos parece igualmente despida de contributo conciliatório entre os regimes em conflito e sobre a possibilidade de os dados serem considerados como uma "*commodity*". Cf. Comissão Nacional de Proteção de Dados, *Parecer/2021/150*, Lisboa, 2021, e *Parecer/2021/100*, Lisboa, 2021.

controlo sobre os seus dados nos mesmos termos comparativamente aquando são (licitamente) tratados para qualquer outra finalidade[66].

Em segundo lugar, do ponto de vista civilístico, os direitos de personalidade (no caso, e em especial, o direito à reserva sobre a intimidade da vida privada), apesar de irrenunciáveis, podem ser voluntariamente limitados, designadamente por contrato — *consentimento vinculante*[67] —, uma vez que "*representam, como direitos subjetivos, posições de liberdade, reconhecidas ao seu beneficiário*"[68], atento também o princípio geral da livre conformação do conteúdo da prestação e do objeto negocial, desde que dentro dos limites da lei e da ordem pública[69]. A limitação voluntária de direitos de personalidade pode visar a exploração económica dos mesmos (que, de resto, não é um fenómeno recente)[70]. Com efeito, e conforme ensina Mafalda Miranda

---

66 De resto, e como salienta Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer, "Data as Counter-Performance – Contract Law 2.0? An Introduction", *ob. cit.*, p. 16, excluir do âmbito da Diretiva 2019/770 os contratos no âmbito dos quais dados pessoais são fornecidos como contraprestação terá como efeito a negação aos respetivos consumidores da proteção oferecida pelas regras de conformidade do serviço ou conteúdo digital aí presentes. Julgamos, por isso, que a procedência do "temor" da AEPD traria acoplado um efeito mais nefasto (a perpetuação da ausência de enquadramento específico desses contratos no seio do direito de consumo) para o consumidor-titular dos dados.

67 Sobre o conceito de *consentimento vinculante* e distinção de figuras afins, cf. Orlando Carvalho (*aut.*), Francisco Liberal Fernandes, Maria Raquel Guimarães, Maria Regina Redinha (*coords.*), *Teoria Geral do Direito Civil*, 4.ª ed., Coimbra, Gestlegal, 2021, p. 207. Para uma análise sobre os limites da autonomia privada em contratos sobre a exploração de direitos de personalidade, cf. Thibault Gisclard, "Limitations of Autonomy of the Will in Conventions of Exploitation of Personality Rights", *in International Review of Intellectual Property and Competition Law* (IIC), Vol. 45, n.º 1 (2014), pp. 18–42.

68 As palavras são de Menezes Cordeiro, *Código Civil Comentado I – Parte Geral*, Coimbra, Almedina, 2020, p. 274, anotação 21.

69 Cf. artigos 81.º, 280.º e 381.º do Código Civil. Cf. Carlos Mota Pinto, António Pinto Monteiro, Paulo Mota Pinto, *Teoria Geral do Direito Civil*, 5.ª ed. reimp., Coimbra, Gestlegal, 2020, p. 101 e 215. Os limites impostos à liberdade contratual pela cláusula geral de ordem pública são objeto de estudo, que recomendamos, em Maria Raquel Guimarães, "A conformação da liberdade contratual pela cláusula geral da ordem pública", *in Derecho y autonomía privada: una visión comparada e interdisciplinar*, LUCÁN, Mª Ángeles Parra (*dir.*); LERA, Silvia Gaspar (*coord.*), Granada, Comares, 2017, pp. 413-434, *maxime* pp. 424- 428, onde a Autora aborda especificamente os limites da limitação contratual de direitos de personalidade.

70 Para um olhar detalhado sobre a limitação voluntária do direito à reserva sobre a intimidade da vida privada, cf. Paulo Mota Pinto, *Direitos de Personalidade e Direitos Fundamentais - Estudos*, 1.ª ed., Coimbra, Gestlegal, 2018, *maxime* pp. 679-716. Cf. em especial, p. 707, onde o Autor reconhece, cabalmente, que a limitação voluntária do direito à reserva sobre a intimidade da vida privada para fins de obtenção de vantagens económicas é possível, sendo "a "*disposição" a título oneroso, ou "comercialização", de informações sobre a vida privada, é, pois, perfeitamente admissível*". Refere ainda o Autor, numa aparente resposta premonitória à posição da AEPD (sendo um texto de 2001), que "*tal "comercialização" de informações sobre a vida privada afigura-se, na verdade, bem distinta, por exemplo, da comercialização de órgãos ou parte do corpo humano* (...). *Não existe, assim, qualquer analogia* [entre as duas situações que permita dar-lhes o mesmo tratamento jurídico]". Por

Barbosa[71], apoiando-se numa construção de Menezes Leitão em torno do instituto do enriquecimento sem causa, aos direitos de personalidade assiste um "*conteúdo de aproveitamento patrimonial, o qual pode funcionar como contrapartida prestacional num contrato que haja sido celebrado*"[72]. Também nesta perspetiva civilística se justifica frisar que a limitação voluntária, e contratual, de direitos de personalidade não se confunde com a sua alienação[73]: o sujeito mantém intacto o controlo sobre os direitos de per-

outro lado, e tomando por base exemplificativa os "*reality shows*", Maria Raquel Guimarães, "A conformação da liberdade contratual...", *ob. cit.*, p. 426, aponta que, atendendo à particularmente expressiva restrição dos direitos à intimidade e à privacidade nessas situações, poder-se-á entender a existência de uma autêntica *alienação* do direito à reserva da vida privada, "*uma renúncia ilícita do seu titular à tutela de um último reduto de intimidade de que a ordem pública não permite dispor*". Sem pretender tomar posição quanto à controvérsia, que escapa ao âmbito do presente texto, sublinhamos ainda assim que, a admitir-se a posição da Autora, será esse um exemplo de violação da cláusula de *ordem pública*, limitativa da restrição voluntária de direitos de personalidade. O fornecimento de dados pessoais como contraprestação, enquanto limitação do direito à reserva da vida privada, não gera, na nossa ótica, uma restrição de direitos de personalidade de escala comparável àquela verificada na participação num "reality show", razão pela qual, por maioria de razão, entendemos que a primeira se deverá considerar aquém da referida fronteira conceptual.

71 Cf. Mafalda Miranda Barbosa, "Negócios onerosos e gratuitos...", *ob. cit.*, p. 1848.

72 Sobre a exploração comercial da imagem, conforme interpretada jurisprudencialmente, cf. Maria Raquel Guimarães, "A conformação da liberdade contratual...", *ob. cit.*, pp. 426-427. É também de referir a anotação 18 ao regime dos direitos de personalidade presente em Menezes Cordeiro, *Código Civil..., ob. cit*, p. 273, onde o Autor classifica o direito ao nome e à imagem como autênticos "*direitos de personalidade patrimoniais*", que "*representam um valor económico, são avaliáveis em dinheiro e podem ser negociados no mercado*". Além desta categoria, o Autor identifica ainda duas outras – direitos de personalidade em sentido forte, que não são comercializáveis (e.g., direito à vida, saúde e integridade corporal), e os direitos de personalidade em sentido fraco, que, dentro de certos limites, podem ter um conteúdo patrimonial (e.g., direito à saúde e à integridade física, "*desde que não sejam irreversivelmente atingidos, nos termos que regem a experimentação humana*"). A identificação e descrição destas duas categorias, por um raciocínio *a contrario*, permite-nos concluir que só em casos pontuais, designadamente quando exista uma irreversibilidade da lesão, se poderá negar o valor patrimonial de um direito de personalidade. Nessa medida, não cremos que o fornecimento de dados pessoais como contraprestação em contratos (que se limita a operar uma limitação na esfera de privacidade do respetivo titular, reversível no momento em que a relação jurídica que a titule cesse, e sempre vinculada aos direitos de controlo conferidos ao titular dos dados pessoais e limites à sua conservação impostos pelo RGPD) tenha dignidade, no campo da proteção da personalidade, que lhe justifique uma tutela de não-comercialização.

73 Václav Janeček, Gianclaudio Malgieri, "Data Extra Commercium", *in* Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (*eds. lits.)*, *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 95-125, não negando a possibilidade de exploração económica de dados pessoais (não constituindo por isso *res*, ou *data*, *extra commercium*), propõe um critério, que nos parece interessante, de "alienabilidade dinamicamente limitada" (*dinamically limited alienability rule*), nos termos do qual só caso a caso, atendendo às regras do RGPD, se poderá determinar se a comercialização de dados pessoais é admissível.

sonalidade que haja limitado, podendo, nos termos do artigo 81.º, n.º 1, do Código Civil, revogar a qualquer momento o acordo limitativo dos mesmos, ainda que possa ter de indemnizar os prejuízos causados à contraparte.

3. A NECESSIDADE PARA A EXECUÇÃO DO CONTRATO COMO FUNDAMENTO DE LICITUDE PARA O TRATAMENTO DE DADOS PESSOAIS

3.1 A SUA *RATIO* E ARTICULAÇÃO COM O PRINCÍPIO DO *PACTA SUNT SERVANDA*

O artigo 5.º do RGPD, tal como vimos, impõe, além de outras obrigações e limites inerentes ao tratamento de dados pessoais, a licitude desse mesmo tratamento (artigo 5.º, n.º, al. a) do RGPD). Esse princípio concretiza-se na necessidade de cada operação de tratamento de dados pessoais ficar coberta por um dos fundamentos de licitude elencados no n.º 1 do artigo 6.º do RGPD. De todos, merecer-nos-á foco, como referido, a necessidade desse tratamento para assegurar a execução de um contrato no qual o titular dos dados seja parte, previsto no artigo 6.º, n.º 1, al. b) do RGPD.

Este fundamento de licitude traduz, em sede de direito da proteção de dados pessoais, o reconhecimento da obrigação que impende sobre o responsável pelo tratamento de cumprir pontualmente os contratos em que é parte[74], sejam estes bilaterais ou unilaterais[75]. O RGPD assume, pois, que a existência de um negócio jurídico, e a necessidade de o cumprir, pode justificar, dentro dos limites naquele definidos, uma limitação ao direito fundamental à proteção de dados do seu titular. Revela, noutra formulação ainda, que o bem jurídico da privacidade não tem a sua supremacia garantida, podendo soçobrar perante outros valores que, *in casu*, se revelem prevalecentes.

Na base[76] desses valores encontra-se, desde logo, a própria autonomia privada do titular dos dados, pois que aceitou contratar conhecendo que (e conformando-se com), cumpridos que fossem os deveres de informação a que o responsável pelo tratamento está obrigado nos termos do artigo 13.º[77] do RGPD, a sua execução implicaria o tratamento dos seus dados pessoais

---

74 Cf. Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation (GDPR): a commentary*, Oxford, Oxford University Press, 2020, p. 330.

75 Cf. A. Barreto Menezes Cordeiro, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, 2021, p. 112.

76 Dizemos estar na base uma vez que a inexistência de um contrato que vincule o titular dos dados exclui, automaticamente e sem necessidade de quaisquer ponderações adicionais em torno da *necessidade para a sua execução*, a hipótese de que o tratamento de dados pessoais se baseie no artigo 6.º, n.º 1, al. b) do RGPD.

77 *Maxime*, conforme já referido, "*a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato,*

de um determinado modo e com determinados limites. Ao celebrar um negócio para a execução do qual o tratamento dos seus dados pessoais é necessário, sabe o titular dos dados que a sua esfera de controlo sobre os seus dados pessoais cede perante o *pacta sunt servanda*, conclusão que é corroborada pela circunstância de não gozar do direito de se opor ao tratamento suportado nesse fundamento de licitude (artigo 21.º, n.º 1, *a contrario*, do RGPD), salvo quando o tratamento tenha por finalidade o *marketing* direto (artigo 21.º, n.º 2 e 3 do RGPD).

3.2. A *NECESSIDADE* PARA A EXECUÇÃO DO CONTRATO. EM ESPECIAL, AS DIRETRIZES 2/2019 DO CEPD.

a) A amplitude do conceito indeterminado

Uma leitura do artigo 6.º, n.º 1, al. b), do RGPD permite, com facilidade, identificar a *necessidade* como o requisito-chave deste fundamento de licitude. Porém, o RGPD não o densifica: não avança, por exemplo, quaisquer critérios para aferir o que se deverá entender como tal, nem distingue entre tipos de necessidade (e.g., uma necessidade operacional, uma necessidade jurídica, uma necessidade económica)[78]. Cumpre, pois, ao aplicador interpretá-lo adequadamente, e tendo em conta a *soft law* interpretativa que haja sido emitida a seu respeito, no sentido de dar ao referido conceito indeterminado a restritividade necessária imposta pela tutela da posição jurídica do titular dos dados, sem, contudo, coartar o racional que terá presidido ao seu desenho pelo legislador europeu.

Neste exercício, importa uma especial menção às Diretrizes 2/2019, emitidas pelo CEPD, através das quais procurou fornecer orientações sobre a interpretação e extensão a dar a este fundamento de licitude no quadro da prestação de serviços da sociedade da informação[79].

---

bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados" (artigo 13.º, n.º 2, al. e) do RGPD).

[78] Discute-se, também, se as obrigações cuja execução é suscetível de ficar coberta por este fundamento de licitude são só as do responsável pelo tratamento ou se, por outro lado, também as do titular dos dados o poderão ser. Não entraremos nessa discussão, uma vez que a tese que defendemos no presente trabalho apoia-se no equilíbrio sinalagmático do contrato globalmente considerado, sendo independente da qualidade do obrigado para efeitos de direito da proteção de dados e das concretas obrigações em causa. Sobre esta matéria, cf. Martin Schmidt-Kessel, "Right to Withdrawn Consent…", *in Data as Counter-Performance…, ob. cit.*, pp. 132-134.

[79] A Diretiva (EU) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação, define estes serviços como "*qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços*" (artigo 1.º, n.º 1, al. b)). É de notar que esta definição não esclarece se o fornecimento de dados pessoais se poderá considerar como "remuneração" para efeitos do preenchimento dos seus re-

Em geral, o CEPD nota que a avaliação sobre a *necessidade* de uma determinada operação de tratamento de dados pessoais não se basta com uma análise sobre se o seu clausulado prevê o tratamento dos dados pessoais. O preenchimento desse conceito deve levar em consideração os valores norteadores e princípios e regras limitativos do tratamento de dados pessoais estabelecidos na lei, em respeito da natureza jusfundamental do direito em causa. Assim — acrescentamos nós —, fica patente que, delimitando o conceito pela negativa, o CEPD exclui do âmbito do artigo 6.º, n.º 1, al. b), do RGPD o tratamento de dados pessoais previsto num dado pacote contratual e que careça de uma conexão fundamental e inerente ao cerne do objeto contratual[80].

Assim, e em linha com anteriores orientações emitidas pelo Grupo de Trabalho do Artigo 29.º[81], o CEPD defende uma interpretação restritiva sobre o que deverá entender-se por *necessário para a execução de um contrato*, excluindo do seu campo de aplicação todas as operações de tratamento de dados pessoais que, não sendo necessárias, sejam impostas unilateralmente ao titular dos dados pelo responsável pelo tratamento, como condição *sine qua non* para a celebração do contrato[82]. Assim, se as mesmas

quisitos. Contudo, o TJUE já decidiu que, pese embora a "remuneração" seja um elemento imprescindível desta definição, a mesma não pressupõe que os serviços sejam financiados necessariamente pelo próprio beneficiário. Cf. Comité Europeu de Proteção de Dados, *Diretrizes 2/2019...*, *ob. cit.*, §3, p. 4, Acórdão *Papasavvas* (Acórdão do Tribunal de Justiça da União Europeia (Sétima Secção), de 11 de setembro de 2014, proferido no âmbito do processo C-291/13), e Acórdão *McFadden* (Acórdão do Tribunal de Justiça da União Europeia (Terceira Secção), de 15 de setembro de 2016, proferido no âmbito do processo C-484/14).

[80] O Comité Europeu de Proteção de Dados, *Diretrizes 2/2019...*, *ob. cit.*, §27, p. 9, aponta como elemento interpretativo o artigo 7.º, n.º 4 do RGPD. Segundo esta entidade, "*esta disposição estabelece, a título ilustrativo, uma distinção entre as atividades de tratamento necessárias para a execução de um contrato e as cláusulas que tornam o serviço subordinado a determinadas atividades de tratamento que não são, de facto, necessárias para a execução do contrato*". Assim, num cenário em que um fornecedor de um serviço digital pago, como um serviço de armazenamento em nuvem, faça depender o fornecimento desse serviço não só ao pagamento do preço, mas também à partilha do seu IP para efeitos de monitorização geográfica dos acessos à *cloud* para fins estatísticos, o tratamento de dados pessoais para este efeito não configura, no entender do CEPD, uma necessidade no âmbito daquele concreto contrato.

[81] Grupo de Trabalho do Artigo 29.º, *Parecer 06/2014 do sobre o conceito de interesses legítimos do responsável pelo tratamento na aceção do artigo 7.º da Diretiva 95/46/CE (WP217)*, adotado em 9 de abril de 2014. Neste Parecer, lê-se, por exemplo, que "... *deve ser interpretada de forma estrita e não abrange as situações nas quais o tratamento não seja verdadeiramente necessário para a execução de um contrato, mas sim imposto unilateralmente à pessoa em causa pelo responsável pelo tratamento. Também o facto de determinado tratamento de dados ser abrangido por um contrato não significa automaticamente que o tratamento é necessário para a execução desse contrato.*"

[82] Pensemos, *e.g.*, no tratamento de dados pessoais para efeitos de integração do cliente na componente social de uma plataforma paga de *streaming* de música, na qual o cliente poderá partilhar as suas audições e interagir com a sua rede de contactos. Levantam especial preocupação as situações de *bundle* de serviços, através das quais o responsável

finalidades puderem ser prosseguidas através de meios alternativos menos invasivos da esfera de privacidade do titular dos dados e que sejam *realisticamente implementáveis*[83], as mesmas não poderão ficar cobertas pelo artigo 6.º, n.º 1, al. b), do RGPD[84].

Gera-se aqui, todavia, a dúvida sobre o que deve considerar-se como uma *alternativa menos intrusiva* e *realisticamente implementável*. A este respeito, deve tomar-se em consideração que, sendo certo que a ponderação da adequação deste fundamento de licitude deve ser realizada em momento anterior à celebração do contrato, é ao controlo da posterior execução deste (melhor, é por referência às operações de tratamento de dados pessoais que se realizem durante a, e no contexto da vigência deste[85]) que a sua proteção se destina. Isto é, esse exercício de ponderação deverá assumir um cenário de efetiva celebração e vigência do contrato, porquanto é precisamente o seu *status* vinculativo, e o regime que lhe é aplicável, que justifica o próprio recurso a este fundamento de licitude. Assim, o exercício de aferição deverá ter por base factual o próprio universo do contrato a celebrar e o seu *objetivo fundamental*[86], tal como percecionado pelo responsável pelo tratamento e por um razoável titular dos dados pessoais — ideia que nos remete para o cumprimento das prestações inseridas no âmbito do sinalagma. Se assim é, tendemos a concluir que a ponderação das alternativas não poderá ignorar os termos em que o clausulado (sobretudo o que compõe o sinalagma) assentará, daí decorrendo que não se deverão considerar como *alternativas menos intrusivas* e *realisticamente implementáveis* aquelas que impliquem uma alteração ao núcleo do programa contratual, sobretudo o que diga respeito aos termos do cumprimento dos deveres de prestação principal, em desrespeito do princípio do cumprimento pontual do contrato.

Cumpre ainda referir o ensinamento de A. Barreto Menezes Cordeiro[87], segundo o qual tem vindo a ser defendido que "*por necessário não se enten-*

---

pelo tratamento agregue num único pacote contratual diferentes serviços, ou diferentes componentes do mesmo serviço, com diferentes contornos e que impliquem o tratamento de dados pessoais para diferentes finalidades. A falta de granularidade dos serviços pode implicar um cruzamento de finalidades entre os diversos serviços ou componentes, ao controlo dos quais o direito sobre a proteção de dados deverá ficar particularmente atento.

83 Cf. Christopher Kuner *et al*, *The EU General Data Protection…*, p. 331.

84 No mesmo sentido, cf. European Data Protection Supervisor, *Opinion 4/2017…*, *ob. cit.,* §52, pp. 14-15.

85 Para efeitos deste trabalho, estamos a desconsiderar, porque irrelevante, os casos em que o fundamento de licitude do artigo 6.º, n.º 1, al. b) do RGPD é utilizado para basear o tratamento de dados pessoais em fase pré-contratual.

86 A expressão é de Grupo de Trabalho do Artigo 29.º, *Parecer 06/2014..., ob. cit.,* recordada por Christopher Kuner *et al*, "*The EU General Data Protection…*", p. 331: "*Assessment of necessity also involves ascertaining the basic purpose of the contract, and this purpose should be identified not just from the controller's perspective but also from the perspective of a 'reasonable data subject' when entering into the contract.*"

87 Cf. A. Barreto Menezes Cordeiro, *Comentário ao Regulamento Geral de Proteção de Dados...*, *ob. cit.*, p. 112.

de, por um lado, indispensável nem, por outro, útil ou vantajoso. O simples facto de desse tratamento resultarem menores custos, temporais ou monetários, para o titular dos dados/cliente, não basta para preencher este requisito". Daqui, ressalta, cremos, uma lição fundamental: a de que o preenchimento do requisito não se basta com a mera atribuição, ao titular dos dados, com o tratamento dos seus dados pessoais, de um benefício (operacional ou económico), no âmbito daquela relação contratual, sendo necessário uma análise mais profunda, atenta a própria lógica interna e dinâmica contratual.

Em qualquer caso, essa análise deverá tomar em consideração a *extra* ou a *intrassinalagmaticidade*[88] do benefício em causa. A mera atribuição de uma vantagem ou utilidade suplementar, não essencial e que não constitua, em si mesma, a vantagem que o titular dos dados visa obter com o dever de prestação principal da contraparte[89], não deverá ser confundida com a necessidade do tratamento para a viabilização deste último, enquanto motor e possibilitador do cumprimento do objetivo jurídico-social do contrato celebrado. Por estar em causa, neste último caso, a própria razão de ser do contrato, a noção de *necessidade* deve ser interpretada num sentido que não comprometa o equilíbrio económico e a justiça do sinalagma assumido, interpretado no contexto da própria lógica e funcionamento económico do contrato em causa.

b) A avaliação da existência, em concreto, de uma "necessidade"

O CEPD propõe, nas Diretrizes 2/2019, as suas orientações que permitem avaliar, no caso concreto, a existência de uma "necessidade" de tratamento de dados pessoais para a execução de um contrato, as quais procuraremos resumir de seguida.

Esta entidade identifica dois momentos no processo de avaliação sobre a existência de uma verdadeira necessidade que permita espoletar a aplicação do artigo 6.º, n.º 1, al. b), do RGPD. *Num primeiro momento*, cumpre ao responsável pelo tratamento *identificar as finalidades*[90] do tratamento em causa. *Num segundo momento*, cumpre-lhe avaliar, objetivamente, se a prossecução das finalidades identificadas depende, *sine qua non*[91], do tratamento de da-

[88] Para uma análise sobre o âmbito do sinalagma, cf. Ribeiro de Faria, *Direito das Obrigações*, vol. I, 2.ª ed., Coimbra, Almedina, 2020, pp. 245-247.

[89] Cf. o mesmo exemplo, acima referido, acerca da componente social de uma plataforma de serviço de *streaming* de música.

[90] As finalidades, uma vez identificadas, devem naturalmente ser especificadas e comunicadas ao titular dos dados, em respeito das obrigações de limitação das finalidades, de transparência do responsável pelo tratamento, de informação e de lealdade para com o titular dos dados pessoais – cf., por exemplo, artigo 5.º, n.º 1, als. a) e b), bem como artigo 13.º do RGPD.

[91] O tratamento de dados pessoais deve, não só se ser suscetível de alcançar a finalidade identificada, como deve ainda constituir a hipótese de ação menos intrusiva e invasiva da esfera de privacidade do titular dos dados. Isto é, se existirem "*alternativas realistas*

dos pessoais. Se o responsável pelo tratamento concluir pela positiva neste segundo momento, as operações de tratamento de dados pessoais que permitam prosseguir as finalidades identificadas (e só essas operações) ficarão cobertas pelo fundamento de licitude estabelecido no artigo 6.º, n.º 1, al. b) do RGPD, em respeito do princípio da limitação das finalidades.

Neste exercício, a necessidade do tratamento para a execução do contrato deve poder ser demonstrada atendendo ao "*objeto contratual fundamental e mutuamente compreendido*"[92] por um titular dos dados razoável. Isto é, o responsável pelo tratamento deverá assegurar-se de que o titular dos dados médio compreende que o *objeto contratual fundamental* implica que a contraparte, enquanto responsável pelo tratamento de dados pessoais, trate os seus dados pessoais de um determinado modo e com determinados limites.

Assim, a CEPD propõe algumas questões a que o responsável pelo tratamento deverá responder e que constituirão um suporte para a avaliação sobre se o artigo 6.º, n.º 1, al. b), do RGPD poderá fundamentar uma concreta operação de tratamento de dados pessoais: (i) qual é a natureza do serviço prestado ao titular dos dados e quais são as suas características distintivas?; (ii) qual é a lógica exata do contrato (ou seja, a sua substância e o seu objeto fundamental)?; (iii) quais são os elementos essenciais do contrato?; (iv) quais são as perspetivas e expectativas mútuas das partes do contrato?; (v) como é promovido ou anunciado o serviço ao titular dos dados?; (vi) um utilizador comum do serviço esperaria de forma razoável que, tendo em conta a natureza do serviço, viesse a ser realizado o tratamento previsto para a execução do contrato de que é parte?

c) As especificidades do tratamento dos dados pessoais para efeitos de publicidade comportamental em linha

De modo a ilustrar a sua interpretação, o CEPD olha de perto sobre a aplicabilidade do artigo 6.º, n.º 1, al. b), do RGPD em certas situações específicas. Uma dessas situações prende-se com o tratamento dos dados pessoais para efeitos de publicidade comportamental (ou personalizada) em linha[93], que constitui (embora não as esgote) uma das finalidades tipicamente associadas ao tratamento de dados pessoais fornecidos enquanto contraprestação em contratos "gratuitos"[94]. Referimo-nos às operações

e menos intrusivas, o tratamento não é «necessário»" à execução do contrato – cf. Comité Europeu de Proteção de Dados, *Diretrizes 2/2019...*, *ob. cit.*, §27, p. 9.

92 Cf. *idem*, §32, p. 10.

93 Para um desenho aprofundado sobre as suas implicações, cf. Grupo de Trabalho do Artigo 29.º, *Parecer 2/2010 sobre publicidade comportamental em linha*, em 22 de junho de 2010.

94 Conforme revela Patrícia Filipa Pereira Carneiro, "*Coisificação" dos dados pessoais..., ob. cit.,* pp. 6 e ss., a expressão económica da publicidade personalizada nos modelos de negócio suportados na economia dos dados é particularmente visível no caso da *Meta* (*Facebook*), que, à data desse texto, revelava ser essa a sua principal fonte de receita.

de monitorização dos comportamentos em linha dos titulares dos dados (o histórico de compras *online*, os *websites* visitados, os "gostos" e partilhas efetuados, entre outros), tendo em vista curar e dirigir ao titular dos dados anúncios talhados ao seu perfil de interesses. A publicidade comportamental, porque suscita questões de particular sensibilidade no direito da proteção de dados — designadamente em matéria de definição de perfis e tomada de decisões automatizadas —, justifica, em alguns aspetos, um regime mais denso, designadamente a Lei n.º 41/2004, de 18 de agosto, que transpôs a Diretiva ePrivacy.

De acordo com a CEPD, "*regra geral*", a publicidade personalizada não constitui um tratamento necessário para a execução de um contrato de serviços em linha, uma vez que se revelaria complexo demonstrar que a execução das obrigações que compõem o núcleo central do objeto contratual depende da publicidade comportamental. Esta ideia, acrescenta o mesmo organismo, é reforçada pelo facto de que, nos termos do artigo 21.º, n.ºs 2 e 3, do RGPD, o titular dos dados mantém o direito de se opor ao tratamento de dados pessoais realizado para finalidades de *marketing* direto.

O CEPD acrescenta que a circunstância de esta publicidade permitir o financiamento (indireto) da prestação do serviço não é suficiente para que, sem mais, se considere a mesma como uma necessidade para a execução do contrato[95]. O mesmo é dizer que a existência de um nexo entre a publicidade comportamental e o financiamento do serviço não constitui uma presunção de necessidade à execução do contrato; ao invés, é necessário testar essa ligação através da resposta às questões acima referidas, e que, em geral, deverão sempre colocar-se.

Do exposto decorre, portanto, que, o CEPD vê com desconfiança que, para finalidades de publicidade comportamental, os dados pessoais sejam tratados com base no artigo 6.º, n.º 1, al. b), do RGPD. Contudo, reconhecendo embora a complexidade da demonstração, não parece excluir à partida a viabilidade da mesma, remetendo a análise para o mesmo teste de viabilidade suportado no questionário que propõe.

[95] Em ligação a esta ideia de que a necessidade para o financiamento indireto de um serviço, por si só, não determina a necessidade do tratamento de dados pessoais, o CEPD aponta também que, em conformidade com Grupo de Trabalho do Artigo 29.º, *Documento de Trabalho 02/2013 dando orientações sobre a obtenção de consentimento para testemunhos de conexão*, adotado em 2 de outubro de 2013, os responsáveis pelo tratamento devem obter o consentimento prévio dos titulares dos dados para colocar os *cookies* necessários para a realização de publicidade comportamental. Cf Comité Europeu de Proteção de Dados, *Diretrizes 2/2019...*, *ob. cit.*, §55, p. 16.

3.3. A PROPOSTA DE UMA INTERPRETAÇÃO ALTERNATIVA. APLICAÇÃO À DIRETIVA 2019/770

Feita esta breve, focada no essencial, incursão sobre a interpretação dada ao fundamento de licitude previsto no artigo 6.º, n.º 1, al. b), do RGPD, cumpre extrair dela algumas considerações dirigidas já para o tema que justifica o presente texto.

Em primeiro lugar, deve reconhecer-se que este fundamento de licitude tem vindo a ser encarado como legitimando aquelas operações de tratamento de dados pessoais que, em termos práticos e operacionais, se revelem necessárias à execução do contrato: é o exemplo do tratamento dos dados pessoais que constituem a morada do titular para efeitos de remessa de uma encomenda efetuada numa loja *online*[96]. Se a ausência de um precedente jurisprudencial[97] que, de um modo evidente, revele a possibilidade de ser interpretado num eixo económico, e não estritamente operacional, provoca no aplicador alguma desconfiança sobre como o interpretar, julgamos dever ser relevada a circunstância de que a letra do RGPD, tal como interpretado pela *soft law* a que nos referimos acima, não se opõe a esta possibilidade[98].

Na verdade, e *em segundo lugar*, as Diretrizes 2/2019 apontam a necessidade de o teste de adequação deste fundamento de licitude ser efetuado

---

96 Martin Schmidt-Kessel, "Right to Withdrawn Consent…", *in Data as Counter-Performance…, ob. cit.*, pp. 132-134, parece referir-se a estes exemplos como operações de tratamento acessórias (*ancillary*), as únicas que, segundo uma interpretação do RGPD, cobertas pelo fundamento de licitude da alínea b) do n.º 1 do artigo 6.º do RGPD. O tratamento de dados pessoais fornecidos como contraprestação não constituiria uma operação de tratamento acessória, razão pela qual, à luz da referida interpretação, não poderia fundar-se no mesmo fundamento de licitude. Ainda que, como refere Martin Schmidt-Kessel, esta distinção possa estar alinhada com a *ratio* que subjazeu à introdução deste fundamento de licitude no direito da proteção de dados pessoais (previamente ao recrudescimento dos modelos de negócio apoiados na economia dos dados), não cremos que esta interpretação tenha cabimento na letra do RGPD (e cuja interpretação não pode ignorar a existência e as especificidades jurídico-contratuais destes modelos de negócio).

97 Sobre o conceito de "necessidade" para efeitos do artigo 7.º, al. f) da Diretiva 95/46/CE, mas sem qualquer contributo relevante para o nosso trabalho, cf. Acórdão *Huber* (Acórdão do Tribunal de Justiça (Grande Secção), de 16 de dezembro de 2008, proferido no âmbito do processo C-524/06) e Acórdão *Rīgas* (Acórdão do Tribunal de Justiça (Segunda Secção), de 4 de maio de 2017, proferido no âmbito do processo C-13/16). Pese embora a escassa relevância, fazemos referência a estas decisões jurisprudenciais porque, entre algumas outras de relevo argumentativo igualmente diminuto, são as elencadas em Comité Europeu de Proteção de Dados, *Diretrizes 2/2019...*, *ob. cit.*, notas 15, 16 e 19, p. 8.

98 Notamos, porém, a reticência de Andreas Sattler, "Autonomy or Heteronomy – Proposal for a two-tier interpretation of Art. 6 GDPR", *in* Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (*eds. lits.)*, *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 241-242, em admitir uma interpretação extensiva deste fundamento de licitude, "descolada" da letra das Diretrizes 2/2019.

em torno do "*objeto contratual fundamental e mutuamente compreendido*". Daqui resultam algumas mensagens dignas de nota: (i) o reconhecimento, por parte do CEPD, da possibilidade de restrição contratual do direito à proteção de dados; (ii) o reconhecimento do papel volitivo e dispositivo do contrato em matéria de proteção de dados pessoais, numa função que nos parece próxima da do consentimento; (iii) o reforço da necessidade de esclarecimento do objeto contratual fundamental, como capacitadora desse mesmo papel volitivo do contrato; e (iv) o reconhecimento de que o funcionamento e lógica interna do *objeto contratual fundamental* assume uma importância decisiva neste exercício de hermenêutica. Assim, a própria teleologia do artigo 6.º, n.º 1, al. b), do RGPD, encontra-se direcionada, ainda que de um modo meramente mediato, para a tutela da execução do contrato e da satisfação do interesse que, através dele, o titular dos dados visou obter – sobretudo tendo, no mesmo ato, concedido no tratamento dos seus dados pessoais, nomeadamente aqueles que haja fornecido como contraprestação.

Em terceiro lugar, a compreensão, pelo titular dos dados, da dinâmica do modelo de negócio do profissional, inclusive (e sobretudo) dos termos do tratamento dos dados pessoais fornecidos como contraprestação, em momento prévio à celebração do contrato, é crucial à determinação da força da declaração negocial do titular dos dados e, por isso, à sustentabilidade d(a necessidade para execução d)o contrato enquanto fundamento de licitude. Assim, só um clausulado *completo*[99], claro e que haja sido efetivamente esclarecido ao titular dos dados, colocando-o a par dos termos em que os dados fornecidos como contraprestação serão tratados, será capaz de munir o consumidor dos instrumentos necessários à formação da sua vontade.

Assim, e em jeito de remate, cremos existir abertura, no RGPD, para que o conceito de *necessidade* do tratamento de dados pessoais para a execução de um contrato abarque outras situações que, não respeitando a aspetos operacionais da execução do contrato[100], ainda assim sejam atendíveis à luz das suas lógicas intrínsecas e dos princípios que os norteiam. Estudaremos, abaixo, o modo como os contratos de fornecimento de conteúdos e serviços digitais a troco de dados pessoais, tal como a Diretiva 2019/770 e o Decreto-Lei n.º 84/2021, de 18 de outubro, os configuram, poderão beneficiar desta abertura, sem, todavia, deixar de sublinhar o esclarecimento pré-contratual do titular dos dados como pedra-de-toque nesta avaliação.

Por último, é importante frisar que o tratamento de dados pessoais fornecidos como contraprestação engloba um vasto universo de realidades. Assim, uma análise conjugada, caso a caso, de elementos como a categoria

---

[99] Não bastando, por isso, o cumprimento do ónus de comunicação e dos deveres de conhecimento, previstos nos artigos 5.º e ss. do Regime das Cláusulas Contratuais Gerais, sobre um clausulado *cherry-picked* que não espelhe toda a realidade do negócio.

[100] Como aqueles que, de resto, e como acima referido, nos parecem permitir preencher a parte final do artigo 3.º, n.º 3, al. b) do Decreto-Lei n.º 84/2021, de 18 de outubro, e o artigo 3.º, n.º 1, *in fine*, da Diretiva 2019/770.

dos dados pessoais a tratar (sobretudo se se tratar de categorias especiais de dados[101]), as especificidades do concreto titular (por exemplo, tratando-se de um menor) ou a finalidade do tratamento (designadamente, como vimos, em caso de publicidade comportamental em linha), será determinante para encontrar, em concreto, o fundamento de licitude mais adequado.

4. A UTILIZAÇÃO DE DADOS PESSOAIS COMO CONTRAPRESTAÇÃO E O SEU REFLEXO NO EQUILÍBRIO CONTRATUAL

Tecidas que estão as considerações que se nos reputam essenciais, do prisma da proteção de dados pessoais, quanto à amplitude do fundamento de licitude previsto no artigo 6.º, n.º 1, al. b), do RGPD, cumpre-nos agora uma reflexão, tomando por base a lei civil portuguesa, sobre o modo como a lógica, funcionamento e regime jurídico inerentes aos contratos de fornecimento de conteúdos ou serviços digitais em que tenham sido fornecido dados como contraprestação, poderão contribuir para suportar o tratamento desses dados como uma condição necessária ao cumprimento do contrato. Com efeito, cremos que a análise sobre se aquele fundamento de licitude cobre, *in casu*, as operações de tratamento de dados pessoais em causa, à luz das Diretrizes 2/2019, depende de uma compreensão prévia sobre a lógica interna do contrato em causa, sobre a conexão entre as prestações que compõem o seu *objeto fundamental,* sobre o papel da monetização dos dados pessoais nesse contexto e, naturalmente, sobre a perceção das partes (*maxime*, do consumidor/titular dos dados pessoais) quanto à sua dinâmica.

4.1 CLASSIFICAÇÃO DO CONTRATO

Um dos aspetos essenciais, e preliminares, deste exercício prende-se com o apuramento da classificação do contrato, enquanto sinalagmático ou não-sinalagmático, por um lado, e enquanto gratuito ou oneroso, por outro. A importância desta etapa é clara: uma compreensão dos contornos mais gerais do contrato permitir-nos-á determinar o regime jurídico aplicável e, a partir dele, dissertar mais a fundo sobre os princípios e valores que o norteiam[102].

---

101 Cf. artigo 9.º do RGPD.

102 Questão não menos importante do que a classificação do contrato enquanto oneroso/gratuito ou sinalagmático/não sinalagmático tem que ver com a sua qualificação no eixo da tipicidade-atipicidade contratual e determinação do respetivo regime. Sobre o tema, que não abordaremos, cf. Rui Pinto Duarte, *Tipicidade a Atipicidade dos Contratos*, Coimbra, Almedina, 2000. Sobre a qualificação dos contratos em que sejam fornecidos dados pessoais como contraprestação, enquanto contratos de compra e venda ou de permuta, cf. Matilde Lopes Bettencourt, "A proteção do consumidor...*", ob. cit.*, p. 432.

a) Contrato sinalagmático ou não-sinalagmático

Sumariamente, o fator de distinção entre estas categorias de contratos prende-se com a circunstância de existir, ou não, um conjunto de obrigações, de ambas as partes, ligadas por um nexo de reciprocidade (o sinalagma) que torne uma dependente da outra. Assim, segundo Menezes Cordeiro[103], um contrato será sinalagmático ou não sinalagmático consoante dê "*lugar a obrigações recíprocas, ficando as partes, em simultâneo, na situação de credores e devedores ou, pelo contrário, apenas facultem uma prestação*". Na noção de Ribeiro de Faria, um contrato será sinalagmático quando dele "*resultam obrigações para ambas as partes*"[104].

Terminologicamente, esta distinção decorre, como se disse, da existência de um sinalagma, que traduz a ideia da "união" entre as obrigações assumidas[105] por ambas as partes contratuais. Dito de outro modo, aquele traduz-se na relação de causalidade, correspetividade e mútua dependência que une ambos os membros da equação contratual[106]. Falamos de *sinalagma genético* quando essa relação se reporta ao momento da celebração do contrato, e de *sinalagma funcional* quando a mesma se "*manifesta e releva durante a vida do contrato, designadamente quanto à simultaneidade do cumprimento*"[107].

A existência de uma união *umbilical* de obrigações justifica, em si mesma, a categorização autónoma de um contrato como sinalagmático, sujeitando-o a um regime jurídico de proteção acrescida em face daquela oferecida aos contratos não-sinalagmáticos – designadamente concedendo às partes do primeiro a possibilidade de recorrerem à exceção de não cumprimen-

---

[103] Cf. Menezes Cordeiro, *Tratado de Direito Civil*, vol. II, 5.ª ed., Coimbra, Almedina, 2021, p. 92. O autor chama ainda a atenção para a imprecisão gerada pela equivalência operada por alguma doutrina, e pela própria lei (cf., por exemplo, artigos 410.º, n.º 2 e 428.º do Código Civil) entre contrato bilateral e sinalagmático, por um lado, e unilateral e não-sinalagmático, por outro. Segundo o Autor, todos os contratos são, no mínimo, bilaterais, porquanto têm mais de uma parte, "*sendo menos correto utilizar depois esses mesmos termos com outro significado*".

[104] Ribeiro de Faria, *Direito das Obrigações*, *ob. cit.*, p. 243, sublinha mesmo, de um modo expressivo, o elemento volitivo que preside à intenção de celebrar um contrato sinalagmático, explicando que as partes *querem* "*apenas obrigar-se num nexo incindível com a obrigação que o outro por sua vez contrai*".

[105] *idem*, p. 246, explica ainda que, em princípio, só os deveres de prestação principal se encontram ligados pelo sinalagma, ainda que, em certos casos, a relação de reciprocidade se possa expandir para deveres secundários de prestação ou deveres de conduta.

[106] *idem*, p. 243, sublinha mesmo, de um modo expressivo, o elemento volitivo que preside à intenção de celebrar um contrato bilateral, explicando que as partes *querem* "*apenas obrigar-se num nexo incindível com a obrigação que o outro por sua vez contrai*". Adiante, *idem*, p. 246, explica ainda que, em princípio, só os deveres de prestação principal se encontram ligados pelo sinalagma, ainda que, em certos casos, a relação de reciprocidade se possa expandir para deveres secundários de prestação ou deveres de conduta.

[107] Cf. Almeida Costa, *Direito das Obrigações*, *ob. cit.*, p. 361, e Ribeiro de Faria, *Direito das Obrigações*, *ob. cit.*, pp. 245 e ss.

to (a que nos referiremos adiante). E assim se justifica porque, apoiado no brocardo latino "*do ut des*", na base do sinalagma está, julgamos, não só a ideia de que uma parte só aceita obrigar-se porque vai igualmente obter um benefício, mas também, e sobretudo, a de que cada parte entende que a própria *medida e substância* da vantagem que irá obter retribui, numa medida justa, o sacrifício que a mesma está disposta a suportar. É essa a razão, por exemplo, que justifica que, citando Ribeiro de Faria[108], "*a ofensa à lei ou aos bons costumes ou a impossibilidade originária de uma das obrigações não deixam confinar os seus efeitos à obrigação a que directamente respeitam, antes estendem a nulidade a todo o contrato bilateral (arts. 280.º e 401.º, 1)*", e que "*o não cumprimento ou um cumprimento defeituoso condiciona o direito à contraprestação*", indiciando o forte "entrelaçamento" entre as obrigações a que se refere o mesmo autor[109].

Ora, cremos que os contratos (logo que bem formados, compreendidos e aceites pelas partes) em que dados pessoais sejam fornecidos como contraprestação pelo fornecimento de serviços ou conteúdos digitais são sinalagmáticos, uma vez que as prestações que compõem o sinalagma estão interligadas por um nexo de causalidade: o profissional só aceita obrigar-se (predispondo, sendo o caso, cláusulas contratuais gerais desenhadas nesse sentido) caso o consumidor forneça os seus dados pessoais, e este só aceita[110] fornecer os seus dados pessoais se obtiver a vantagem de benefi-

---

108 Cf. Ribeiro de Faria, *Direito das Obrigações*, *ob. cit.*, p. 245 e p. 248, respetivamente.

109 Numa perspetiva interessante, Maria de Lurdes Pereira, *Conceito de prestação e destino da contraprestação*, Coimbra, Almedina, 2001, pp. 110 e ss., estuda o reflexo da interdependência das obrigações sinalagmáticas no regime do artigo 795.º do Código Civil. Sobre a impossibilidade da prestação, cf. Catarina Monteiro Pires, *Impossibilidade da Prestação*, reimp., Coimbra, Almedina, 2020.

110 Questão relevante, mas distinta (a qual já antecipámos anteriormente e afloraremos adiante), tem a ver com a própria perceção do consumidor de que que está não só a fornecer dados pessoais que servirão como contraprestação da vantagem que irá obter através do contrato, mas também de que o profissional os irá, depois, tratar – no fundo, a perceção de gratuitidade destes serviços, a que nos referimos no capítulo introdutório deste trabalho. Em nosso entender, porém, essa discussão coloca-se, em termos lógicos, a montante da classificação do contrato enquanto sinalagmático ou não sinalagmático e com ela não contende: com efeito, para a categorização do contrato releva o conteúdo contratual propriamente dito, presumidamente bem formado e sem prejuízo da relevância da vontade das partes como elemento interpretativo do mesmo, nos termos gerais. Todavia, vale desde já salientar que, tratando-se de cláusulas contratuais gerais cujo conteúdo não haja sido devidamente exposto ao aceitante nos termos dos artigos 5.º e ss. do Regime das Cláusulas Contratuais Gerais, as mesmas poderão ser consideradas excluídas dos contratos singulares em que foram apostas, com o risco de nulidade destes, caso a exclusão implique "*uma indeterminação insuprível de aspetos essenciais ou um desequilíbrio nas prestações gravemente atentatório da boa fé*" (artigo 9.º, n.º 2). Daí, o esclarecimento do consumidor, além de se tratar de um elemento fundamental no exercício de avaliação sobre a necessidade do tratamento dos seus dados pessoais para a execução do contrato nos termos acima expostos, terá, necessariamente, impacto no apuramento do seu real clausulado e, a jusante, na classificação e validade do acordo.

ciar do conteúdo ou do serviço. Ambas as partes se assumem, no contrato, simultaneamente como credora e devedora[111].

b) Contrato gratuito ou oneroso

Diversamente da distinção anterior, a característica distintiva desta classificação prende-se, não com a atribuição de obrigações recíprocas às partes, mas com a circunstância de o contrato implicar atribuições patrimoniais para uma ou ambas as partes[112]. Assim, Ribeiro de Faria[113] nota que, nesta distinção, "*o que avulta é o conteúdo e a finalidade do negócio, o que está em causa é a função económica do contrato, do que se trata é determinar as atribuições patrimoniais que dele resultam*", sendo um contrato oneroso "*se existirem atribuições patrimoniais de ambas as partes, desde que, debaixo do ponto de vista destas, haja uma equivalência ou equilíbrio entre as prestações efetuadas*". Em sentido próximo, Mota Pinto[114], refere que "*os negócios onerosos ou a título oneroso pressupõem atribuições patrimoniais de ambas as partes, existindo, segundo a perspectiva destas, um nexo ou relação de correspectividade entre as referidas atribuições patrimoniais*", ensinando o mesmo autor que os negócios gratuitos se caracterizam "*pela intervenção de uma intenção liberal (animus donandi, animus beneficiandi)*"[115].

---

[111] Devemos chamar à atenção que não é pacífico que o consumidor-titular dos dados se obrigue, efetivamente, a fornecer dados pessoais. Sobre o tema, cf. Axel Metzger, "A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services", *ob. cit.*, pp. 36-39. Não pretendendo aprofundar o tema, diremos apenas que, atenta a liberdade de exploração económica de direitos de personalidade, nos termos aprofundados no nosso trabalho, não vemos nenhuma razão para que, dentro desses limites, os dados pessoais não possam integrar o objeto contratual e, logo, o seu titular ficar obrigado ao complexo obrigacional tendente ao seu fornecimento ao profissional. Assim, será a interpretação do concreto clausulado contratual a dar a resposta sobre se, *in casu*, estamos perante uma obrigação do titular dos dados ou de uma vinculação de outra espécie, porventura ajurídica. Para o nosso exercício, por isso, tomamos por base a qualificação destes contratos como sinalagmáticos porque, ao nível académico, cremos que essa classificação é efetivamente possível (sendo ainda certo que, na prática, não vemos razões para que os prestadores de serviços "gratuitos", enquanto predisponentes das cláusulas contratuais gerais que constituem os contratos em tese, não procurem efetivamente vincular o consumidor-titular dos dados a obrigações jurídicas).

[112] A classificação do contrato determinará, por exemplo, o sentido em que a declaração negocial deverá ser interpretada, nos termos do artigo 237.º do Código Civil, ou a possibilidade de recurso à ação de impugnação pauliana, prevista nos artigos 610.º e ss. do Código Civil. Para uma súmula mais completa das diferentes abordagens possíveis acerca da distinção entre contratos gratuitos e onerosos, cf. Mafalda Miranda Barbosa, "Negócios onerosos e gratuitos...", *ob. cit.*, pp. 1810 e ss.

[113] Cf. Ribeiro de Faria, *Direito das Obrigações*, *ob. cit.*, pp. 253-254.

[114] Cf. Carlos Mota Pinto, António Pinto Monteiro, Paulo Mota Pinto, *Teoria Geral...*, *ob. cit.*, p. 400.

[115] Sobre o nexo da equivalência, cf. tb. Francisco Manuel de Brito Pereira Coelho, *Contratos Complexos e Complexos Contratuais*, 1.ª ed., Coimbra, Coimbra Editora, 2014, pp. 145 e ss.

Por outro lado, Pais de Vasconcelos parece focar o cerne da distinção no jogo de contrapartidas objetivamente considerado: "*os contratos onerosos são aqueles em que é estipulado um sistema de contrapartidas",* unido por um nexo de correspetividade e equilibrado na perspetiva das partes*,* entendendo, por seu turno, os gratuitos como aqueles *"em que à prestação principal não corresponde uma contrapartida, em cujo conteúdo se estipula uma atribuição patrimonial unilateral*"[116]. O equilíbrio entre as contrapartidas de um contrato oneroso, porém, não tem necessariamente de corresponder a uma simetria efetiva e fáctica entre as prestações integrantes do sinalagma (diríamos, um equilíbrio *objetivo*), antes bastando que traduza uma equivalência relativa, perseguida e aceite contratualmente pelas partes, de acordo com as suas próprias valorações subjetivas, nas concretas circunstâncias de facto em que se apoiou a celebração do negócio (equilíbrio *subjetivo*)[117]. Assim, se à celebração de um negócio tiver presidido um *animus donandi*, o mesmo ter-se-á como gratuito; se, ao invés, as partes pretenderam atribuir à contraparte uma vantagem causalmente vinculada à vantagem que elas mesmas obtêm do contrato, estaremos perante um contrato oneroso[118].

Ora, atentas as especificidades e implicações jurídicas de uma contraprestação sob a forma de dados pessoais, inerentes à sua proteção enquanto direito de personalidade e direito fundamental, revela-se complexo determinar a qualificação dos contratos em consideração[119]. Com efeito, se a ausência de

---

[116] Cf. Pedro Pais de Vasconcelos, Pedro Leitão Pais de Vasconcelos, *Teoria Geral..., ob. cit.,* p. 451 e Pedro Pais de Vasconcelos, *Contratos atípicos*, 2.ª ed., Coimbra, Almedina, 2009, pp. 140 e ss. e 378 e ss.

[117] Adotamos uma posição alinhada com aquela que parece resultar de Carlos Mota Pinto, António Pinto Monteiro, Paulo Mota Pinto, *Teoria Geral..., ob. cit.,* p. 401 e Mafalda Miranda Barbosa, "Negócios onerosos e gratuitos...", *ob. cit*., pp. 1815 e ss. Neste último escrito, a Autora salienta que do que se trata aqui é de um *subjetivismo mitigado*, explicando que "*não se sindicam intenções ocultas ou segundas intenções. Não se exige, para que o negócio seja qualificado como gratuito, que a atribuição patrimonial corresponda a um ato de altruísmo. O sujeito que atribui uma vantagem a outrem, não sendo compensado com uma contraprestação equivalente, pode fazê-lo por motivos egoístas. (...) Mas a intenção não pode ser oculta num outro sentido. De facto, implicando a qualificação e classificação do negócio jurídico, qualquer que ele seja, um prévio trabalho interpretativo, havemos de nos guiar pelo artigo 236.º CC. O que nos importa, portanto, é saber qual o sentido que um declaratário normal, colocado na posição do real declaratário, teria retirado da declaração de vontade. (...) A diferença está, portanto, entre a vontade e a motivação, não sendo esta relevante.*"

[118] Vale precisar e sublinhar que o critério fundamental para classificar um contrato como oneroso ou gratuito prende-se com a *intenção* das partes ao momento da sua celebração, e não com os efeitos objetivos do negócio no património das partes. Conforme ensina Menezes Cordeiro, "*um negócio pode vir a revelar-se como imensamente lucrativo para uma das partes e ruinoso para a outra; nem por isso haverá gratuitidade: se as partes o não tiverem querido como tal, antes se verificará a presença de um negócio (oneroso) em desequilíbrio*". Cf. Menezes Cordeiro, *Tratado de Direito Civil*, vol. II, *ob. cit.*, p. 107.

[119] Apesar das importantes implicações que esta classificação tem, ainda hoje, ao nível do regime aplicável, é, em nosso entender, uma fronteira cada vez mais artificial e que não permite responder com exatidão e clareza a várias realidades geradas pela dinâmica do

um dispêndio pecuniário por parte do consumidor pode indiciar a gratuitidade do negócio[120], a verdade é que esta análise não pode ignorar o valor económico dos dados pessoais[121]. Existem, em nosso entender, argumentos suficientes no sentido de demonstrar a onerosidade destes negócios.

Em primeiro lugar, e tal como ensina Mafalda Miranda Barbosa[122], a delimitação do campo de aplicação da Diretiva 2019/770 e do Decreto-Lei n.º 84/2021, de 18 de outubro, tem como ponto de partida e pressuposto a onerosidade dos contratos de fornecimento de conteúdos e serviços digitais, aplicando-se quando o "*consumidor pague ou se comprometa a pagar o respetivo preço*" (cf., respetivamente, artigo 3.º, n.º 1, e artigo 3.º, n.º 3, al. a))[123]. É em torno desse pressuposto que são estabelecidas as normas sobre a conformidade dos conteúdos ou serviços digitais, responsabilidade do profissional e meios de ressarcimento em caso de não fornecimento ou falta de conformidade do forne-

comércio, capaz de nos demonstrar a existência de contratos que não se enquadram de um modo claro em qualquer uma das figuras de acordo com as suas conceções clássicas (pensemos, por exemplo, num contrato de prestação de serviços mútua, em que nenhuma das partes sofre um verdadeiro incremento ou dispêndio patrimonial ou pecuniário, ou num contrato de compra e venda em que a coisa é vendida por um preço meramente simbólico). Por essa razão, importa encarar este conceptual com a necessária e suficiente elasticidade, sob pena de não permitir a catalogação de inúmeros modelos contratuais factualmente praticados e, com isso, deixar indefinido o seu regime. Cf. Pedro Pais de Vasconcelos, Pedro Leitão Pais de Vasconcelos, *Teoria Geral do Direito Civil*, 9.ª ed. reimp., Coimbra, Almeida, 2022, p. 451.

120 Ou, pelo menos, indiciar a perceção, por parte do consumidor, de que o conteúdo ou o serviço digital em causa é fornecido a título de liberalidade, de acordo com o mecanismo de interpretação plasmado no artigo 236.º do Código Civil. Por outro lado, a este respeito, e apesar de tal não merecer dúvidas, Hervé Jacquemin chama a atenção de que a circunstância de a contraprestação assumir a forma de dados pessoais e não de dinheiro não impacta com a existência de um vínculo contratual. Cf. Hervé Jacquemin, "Contracting Around Privacy…", *ob. cit.*, p. 37.

121 De resto, a própria Comissão Europeia já manifestou que "[d]*ado o aumento do valor económico dos dados pessoais, esses serviços não podem ser considerados como «gratuitos»*". Cf. Proposta de Diretiva do Parlamento Europeu e do Conselho, que altera a Diretiva 93/13/CEE do Conselho, de 5 de abril de 1993, a Diretiva 98/6/CE do Parlamento Europeu e do Conselho, a Diretiva 2005/29/CE do Parlamento Europeu e do Conselho e a Diretiva 2011/83/UE do Parlamento Europeu e do Conselho, a fim de assegurar uma melhor aplicação e a modernização das normas da UE em matéria de defesa do consumidor, COM/2018/185 final – 2018/0090 (COD), p. 3. Sobre o valor económico dos dados pessoais e a sua comparação, distinção e articulação com a noção de "preço", cf. Matilde Lopes Bettencourt, "A proteção do consumidor...", *ob. cit.*, p. 429, bem como Philipp Hacker, "Regulating the Economic Impact of Data as Counter-Performance...", *ob. cit.*, pp. 48 e ss.

122 Cf. Mafalda Miranda Barbosa, "Negócios onerosos e gratuitos...", *ob. cit*., pp. 1840 e ss.

123 Reconheça-se que a própria Diretiva 2019/770, no seu considerando 12, deixa ao direito nacional a qualificação jurídica dos contratos, enquanto, por exemplo, contrato de compra e venda, de prestação de serviços, de aluguer ou outro. Contudo, ainda assim este indício parece-nos importante, uma vez que revela a intenção que presidiu à definição da disciplina jurídica prevista nessa diretiva e que, grosso modo, foi estendida aos contratos em que o pagamento é efetuado com o fornecimento de dados pessoais.

cimento, entre outros aspetos – disciplina que não nos parece compatível com o espírito de liberalidade inerente aos contratos gratuitos[124]. Nessa medida, a extensão da mesma disciplina, com pontuais adequações[125], aos contratos com fornecimento de dados pessoais como contraprestação constitui um forte argumento no sentido de que um pagamento com dados pessoais ao invés de dinheiro não altera a qualificação do contrato como oneroso.

Em segundo lugar, nestes novos modelos contratuais o cliente, limitando voluntariamente o "*direito de personalidade, permitindo que* [o] *terceiro tenha acesso a um círculo de reservas*"[126], apesar de não se obrigar a uma prestação pecuniária, obriga-se, ainda assim, a fornecer um bem com valor transacionável e suscetível de gerar um incremento patrimonial na esfera jurídica do credor. Do ponto de vista objetivo[127], assiste-se, pois, à compensação patrimonial, ainda que indireta, das prestações que compõem o sinalagma, o que concorre para a classificação do negócio como oneroso[128].

4.2 A PROTEÇÃO DA EQUIVALÊNCIA DAS PRESTAÇÕES INTEGRADAS NO SINALAGMA

No cume da lista de princípios fundamentais que enforma o direito das obrigações surge o princípio da autonomia privada[129] (artigo 405.º do Código Civil), do qual resulta que, na sua aceção de liberdade contratual,

---

124 Veja-se, por exemplo, o regime do contrato de doação (artigo 940.º e ss. do Código Civil), enquanto padrão de contrato gratuito. A transmissão de um direito ou coisa onerada ou viciada não gera, em princípio, responsabilidade para o doador, apesar de assistir um direito de anulação do negócio ao donatário (artigo 957.º do Código Civil).

125 Por exemplo, no que diz respeito à possibilidade de resolução do contrato em caso de fornecimento de um conteúdo ou serviço digital com uma falta de conformidade menor (artigo 14.º, n.º 6, da Diretiva 2019/770 e artigo 37.º, n.º 5, do Decreto-Lei n.º 84/2021).

126 Cf. Mafalda Miranda Barbosa, "Negócios onerosos e gratuitos...", *ob. cit*., p. 1843.

127 Também neste ponto é de relembrar a questão da (não) perceção das partes quanto ao equilíbrio das prestações. Do ponto de vista do profissional, não temos dúvidas de que este planeia o seu modelo de negócio com a expectativa de poder vir a ser compensado através da monetização dos dados pessoais que receber, inexistindo por isso qualquer *animus donandi* na sua prestação. Por outro lado, do ponto de vista do consumidor médio, poderá existir a convicção da gratuitidade daquela prestação. Todavia, e tal como Mafalda Miranda Barbosa, "Negócios onerosos e gratuitos...", *ob. cit*., p. 1850, não cremos que essa diferença informacional contenda com a classificação do contrato como oneroso, sem prejuízo de indiciar, naturalmente, uma necessidade de reforço dos deveres de informação e transparência.

128 Segundo Juliette Sénéchal, "Article 16(2) of the 'Digital Content and Digital Services' Directive on the Consequences of Termination of Contract, or the Difficult Articulation between Union Law on Consumer Contract and Union Law on the Protection of Personal Data", *in* Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (*eds. lits.)*, *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 157-160, a jurisprudência francesa tem sido lapidar em considerar estes contratos como onerosos.

129 Cf. Almeida Costa, *Direito das Obrigações*, 12.ª ed. reimp., Coimbra, Almedina, 2020, p. 113.

cada sujeito jurídico, dentro dos limites traçados pela lei, goza da faculdade de, através da celebração de contratos[130], cooperar com terceiros, de modo a satisfazer necessidades, de qualquer natureza (patrimonial, moral, pessoal), obtendo e/ou concedendo vantagens de um modo juridicamente tutelado. Daqui decorre, por isso, que, dentro dos mesmos limites, cada sujeito é livre de, obrigando-se a si mesmo a adotar certo comportamento, restringir a sua própria esfera de liberdade para atribuição de um benefício a terceiros[131].

É este, parece-nos, o efeito jurídico primacial da celebração de um contrato, enquanto modalidade de negócio jurídico, apoiado no reconhecimento e conformação, pelas partes, de que, dali em diante, estarão vinculados a determinados comportamentos, e pelo qual serão responsáveis[132]. Com efeito, o princípio geral que assegura a razão de ser de um contrato é o do seu cumprimento pontual e de boa-fé (artigos 406.º e 762.º do Código Civil), que determina que, em princípio, não poderá ser unilateralmente modificável ou revogável.

a) A especial tutela do pacta sunt servanda num contrato sinalagmático

Sendo certo que o *pacta sunt servanda* é um princípio basilar e comum a qualquer contrato[133], sem prejuízo das suas exceções, é no regime dos contratos sinalagmáticos que revela toda a sua força e amplitude. Para que se consiga compreender a profundidade da tutela do sinalagma, importa atentar àquela que é a manifestação mais sonante do regime do contrato sinalagmático: a exceção de não cumprimento (artigos 428.º a 431.º do Código Civil)[134].

---

130 Enquanto, na aceção de Carlos Ferreira de Almeida, *Contratos,* vol. I, 7.ª ed., Coimbra, Almedina, 2022, p. 34, "*acordo formado por duas ou mais declarações que produzem efeitos jurídicos conformes ao significado do acordo obtido*".

131 Nas palavras de Carlos Ferreira de Almeida, *Contratos,* vol. I, *ob. cit.*, p. 35, "*onde vigora o princípio da liberdade contratual (artigo 405.º), o acordo entre quaisquer pessoas pode, salvo limitações legais, ter como efeito a alteração de quase todas as situações jurídicas de que qualquer delas é titular, nos precisos termos do acordo que entre si estabeleceram*". Sobre a distinção entre autodeterminação e autonomia privada, cf. Joaquim de Sousa Ribeiro, *O Problema do Contrato - As Cláusulas Contratuais Gerais e o Princípio da Liberdade Contratual*, Coimbra, Almedina, 1999, pp. 21 e ss.

132 Cf. Joaquim de Sousa Ribeiro, *O Problema do Contrato..., ob. cit*, pp. 63 e ss.

133 Ainda assim, em certas circunstâncias, a lei admite exceções ao princípio *pacta sunt servanda*, sendo o exemplo mais paradigmático o do regime da alteração superveniente das circunstâncias, previsto no artigo 437.º do Código Civil. Com particular interesse para o presente texto destacamos a exceção imposta pelo artigo 81.º, n.º 2 do Código Civil, que determina a liberdade, e a todo o tempo, de revogação de um contrato pela parte que, através dele, tenha limitado os seus direitos de personalidade.

134 O Código Civil oferece outros institutos especialmente desenhados como tutela do equilíbrio do sinalagma, como seja a invalidade do negócio em caso de impossibilidade originária ou da ilicitude de uma das prestações (artigo 401.º, n.º 1) ou a exoneração do credor da contraprestação e o direito de repetir o que já tenha satisfeito em caso de impossibilidade superveniente (artigo 795.º, n.º 1 do Código Civil). Cf. Almeida Costa, *Direito das Obrigações*, *ob. cit.*, p. 366.

Nos termos do artigo 428.º do Código Civil, a existência de um sinalagma justifica que um devedor possa recusar o cumprimento da sua obrigação[135] enquanto a contraparte não cumprir a sua ou assegurar o cumprimento simultâneo, salvo existindo prazos diferentes para o cumprimento das prestações[136]. O artigo 429.º do Código Civil vai ainda mais longe nesta tutela, ao conferir às partes a faculdade de, mesmo que obrigadas a cumprir em primeiro lugar, recusar fazê-lo enquanto a contraparte não cumpra ou garanta cumprir, caso, posteriormente à celebração do contrato, se verifique alguma circunstância que implique a perda do benefício do prazo (artigos 780.º a 782.º e 934.º do Código Civil). Estas circunstâncias prendem-se, em suma, com o risco de que o cumprimento da contraprestação possa estar comprometido, designadamente em virtude do deterioramento da situação económica do obrigado[137].

O objetivo fundamental desta figura é claro: compelir a contraparte a respeitar o sinalagma. Uma reflexão sobre o mesmo revela-nos as ideias centrais que lhe estão na base, e das quais se extraem princípios que exprimem a extensão da proteção jurídica do sinalagma. Com efeito, no cerne da figura encontra-se uma certa ideia de garantia, suportada na própria prestação do credor (mais visível e palpável quando se trata de uma obrigação pecuniária, embora não se circunscreva a esses casos), contra os danos gerados pelo potencial incumprimento da contraparte.

Dito de outro modo, a exceção de não cumprimento demonstra o reconhecimento, por parte da lei, de que o *ground zero* da celebração de um contrato sinalagmático reside na confiança, de ambas as partes, de que o cumprimento do ciclo sinalagmático as deixará economicamente indemnes[138], sendo-lhes inexigível que, perante o risco de quebra desse equilíbrio pela contraparte, empreguem os seus esforços na execução daquele contrato até que tal risco sucumba[139]. Assim, caso se consume um inadimplemento,

---

135 Vale sublinhar que o direito concedido pela exceção de não cumprimento não deve ser confundido com uma dissolução do vínculo contratual, que permanece intacto nos precisos termos contratados.

136 Almeida Costa chama a atenção para a necessidade de se interpretar corretivamente o texto desta norma. Num cenário em que existam, efetivamente, prazos diferentes para o cumprimento, só o devedor que haja de cumprir em primeiro lugar fica impedido de opor a exceção de não cumprimento. Cf. Almeida Costa, *Direito das Obrigações*, *ob. cit.*, p. 365.

137 A doutrina discute se a exceção de não cumprimento pode operar em casos não previstos no artigo 780.º do Código Civil. Cf. Almeida Costa, *Direito das Obrigações*, *ob. cit.*, p. 365, nota 3, e Ribeiro de Faria, *Direito das Obrigações, ob. cit.*, p. 250.

138 A confiança das partes de que um contrato sinalagmático as não deixará numa situação de prejuízo económico não se gera, naturalmente, num contrato aleatório, em que o esse risco constitui uma parte fundamental do próprio objeto contratual. Não é, porém, esse o cenário que estamos a assumir na nossa análise.

139 Assim, Menezes Leitão, *Direito das Obrigações*, vol. I, 16.ª ed., Coimbra, Almedina, 2022, p. 200, ensina que da lei decorre "*uma interdependência entre as duas prestações, que se deve manter durante toda a vida do contrato, estabelecendo-se por isso que uma pres-*

a parte "fiel" que tenha recorrido à exceção de não cumprimento terá já evitado parte dos danos causados na sua própria esfera jurídica (sem prejuízo do ressarcimento, em sede de ação de responsabilidade contratual, dos que demais houver a indemnizar); terá ainda evitado a atribuição de uma vantagem injustificada à parte inadimplente causalmente ligada à medida do seu sacrifício (também ele, pois, injustificado)[140], e que, em última análise, haveria de ser reposta com recurso à figura do enriquecimento sem causa (artigo 473.º e ss. do Código Civil).

Aqui chegados, cremos estar em posição de tecer a seguinte conclusão: num contrato sinalagmático, o cumprimento de uma obrigação compreendida no sinalagma, mais do que uma *condição volitiva* do cumprimento da contraprestação, é reconhecido pela lei como um *pressuposto jurídico-económico* para o cumprimento da correspondente[141]. Sem ela, a parte achar-se-ia numa posição de cumprimento prejudicial à sua própria esfera jurídica, inexigível, como vimos, pelo Código Civil, princípio que, se admitido, poria não só em risco o equilíbrio económico do contrato em causa, como, num caso extremo, seria suscetível de colocar em risco a própria subsistência económica da parte em prejuízo.

b) O equilíbrio das (justas) prestações sinalagmáticas

Na base da especial tutela conferida aos contratos sinalagmáticos, a que acima aludimos, encontra-se, em nosso entender, o respeito pelos princípios da proporcionalidade contratual e do equilíbrio das prestações[142]. Segundo Brandão Proença, o princípio da proporcionalidade "*repousa na ética aristotélica, tomista e jusnaturalista, envolve uma ideia de ponderação (Angemessenheit) entre bens/interesses conexionados (por ex., entre os benefícios de um e os sacrifícios de outro (...)), entendendo-se como sua proposição nuclear a máxi-*

tação não deve ser executada sem a outra e que, se uma das prestações se impossibilitar, a outra também se deve extinguir", situação que o autor descreve como sinalagma funcional.

140 Lógica que, de resto, se transplanta para os contratos gratuitos, aos quais preside um *animus donandi* e que se traduz no enriquecimento patrimonial do beneficiário na medida do empobrecimento do obrigado. Não será assim, contudo, em todos os casos (e.g., doação onerosa, artigo 963.º do Código Civil).

141 Temos uma posição próxima da de Menezes Leitão, *Direito das Obrigações*, vol. I, *ob. cit.*, p. 200: "*o fundamento* [do sinalagma] *não reside, porém, na convenção tácita das partes, mas antes numa exigência de justiça comutativa que veda o desequilíbrio contratual que seria gerado pela realização apenas de uma das prestações, sem que a outra fosse igualmente realizada*".

142 Vale referir que a autonomia dos princípios da proporcionalidade contratual e do equilíbrio das prestações não é unânime na doutrina portuguesa. Acompanhamos, porém, Brandão Proença, que reconhece a relevância deste princípio na dogmática hodierna. Cf. Brandão Proença, "Da «justa medida» (proporcionalidade) no Título I (das obrigações em geral) do Livro II do Código Civil de 1966.*", in Estudos de Direito das Obrigações. Contrato-promessa. Responsabilidade civil. Da proporcionalidade obrigacional,* Porto, Universidade Católica Editora, 2018, p. 139.

ma aristotélica segundo a qual "o justo é o proporcionado e o injusto é aquilo que não respeita a proporção"[143]. É precisamente em respeito dessa ideia de equilíbrio entre prestações que se compreende, cremos, a figura da exceção de não cumprimento, como reflexo de que uma obrigação assumida num contrato sinalagmático encontra o seu fundamento e a razão da sua medida, precisamente, no fundamento e na medida da contraprestação.

Verifica-se, assim, uma especial sensibilidade do ordenamento jurídico para com o equilíbrio e justiça prestacionais, valores em que assenta o sinalagma: se um contrato não-sinalagmático gera, na esfera da parte beneficiária, uma confiança juridicamente tutelada de que as prestações serão cumpridas nos termos acordados[144], aquela gerada por um contrato sinalagmático radica ainda na expectativa de que o investimento económico empenhado pela parte fiel será protegido pelo retorno que a mesma obterá pelo cumprimento pontual da contraparte. É esta expectativa uma decorrência lógica da ideia de que, e nas palavras de Menezes Cordeiro, "*o Direito tutela (e cristaliza) o negócio jurídico pela necessidade de proteger a confiança que ele suscita nos destinatários e, em geral, nos participantes na comunidade jurídica. Tendo, voluntariamente, dado azo ao negócio, o declarante não pode deixar de ser responsabilizado por ele*"[145].

Tudo somado, concluímos que a lei reconhece o princípio geral da inexigibilidade de que uma parte suporte o esforço inerente ao cumprimento das obrigações assumidas num contrato sinalagmático, a menos que, em respeito da sua justiça e equilíbrio, a contraprestação (independentemente da sua espécie ou natureza, desde que dentro dos limites da lei) não esteja em risco de ser incumprida. Se assim é, o fornecimento de dados pessoais, nos contratos em apreço, assume-se como a justa (porque mutuamente querida) retribuição pelo esforço económico do prestador do conteúdo ou serviço digital, sendo aquele economicamente necessário a este. Recordando as posições já assumidas pelo TJUE (cf. Acórdãos *Papasavvas* e *McFadden*), em situações paralelas à do caso que aqui analisamos, esta circunstância não retira a qualificação dos "serviços gratuitos" como "serviços da sociedade da informação", nem os negócios subjacentes como sinalagmáticos e/ou onerosos.

É preciso atentar ainda que, na dinâmica típica desses contratos, rigorosamente, os dados pessoais fornecidos como contraprestação não servem, eles próprios e sem mais, como o correspetivo económico direto que remunera a prestação do profissional: a riqueza é gerada a jusante, através dos procedimentos de tratamento dessa informação. Nessa medida, a existência de um nexo entre o fornecimento do conteúdo ou do serviço digital e os dados pessoais do consumidor não deve ser estendido, sem

---

143 Cf. Brandão Proença, "Da «justa medida» (proporcionalidade)...", *ob. cit*, pp. 142 e 143.

144 E cujo incumprimento é suscetível, naturalmente, de gerar danos. Pense-se, por exemplo, num caso de incumprimento de mandato.

145 Cf. Menezes Cordeiro, *Tratado de Direito Civil*, vol. II, 5.ª ed., Coimbra, Almedina, 2021, p. 57.

mais, ao tratamento desses dados, para efeitos de recurso ao fundamento de licitude previsto no artigo 6.º, n.º 1, al. b), do RGPD. Essa avaliação deverá ser efetuada caso a caso, à luz das especificidades de cada parte, no contexto de cada contrato e sempre em articulação com as Diretrizes 2/2019.

5. O PAPEL DO DIREITO DO CONSUMIDOR NA (JUSTA) FORMAÇÃO DO CONTRATO E NA COMPOSIÇÃO DO SEU OBJETO

Na base da formação de um contrato, enquanto reflexo por excelência da autonomia negocial, está, sabemo-lo bem, o encontro de duas declarações negociais complementares - a proposta e a aceitação, que mais não são do que a receção jurídica da vontade *real* das partes contratantes, enquanto pessoas jurídicas dotadas de capacidade negocial. No quadro do direito civil português, essa vontade pode, regra geral, ser expressa por qualquer modo, sem que tal prejudique a efetiva celebração do contrato assim que as duas declarações de vontade se cruzem (artigo 219.º do Código Civil)[146].

Esta premissa lógica, porém, pressupõe que as declarações de vontade hajam sido emitidas no contexto de um modelo de contratação em que as partes se encontrem em planos negociais equivalentes e possam, com o mesmo grau de esclarecimento e liberdade, disputar o conteúdo contratual e decidir contratar[147]. Contudo, em certas situações, designadamente motivadas por um desequilíbrio económico das partes, esta equivalência não é um dado adquirido: nestes casos, a declaração negocial poderá não traduzir (ou não traduz de facto), de um modo *juridicamente confiável*, a vontade *real* do declarante, não se encontrando uma verdadeira autonomia negocial. Para corrigir estas situações, o legislador estabeleceu um conjunto de regras e institutos destinados a assegurar, em suma, o devido esclarecimento do declarante em relação à matéria sobre a qual está a declarar e a liberdade dessa declaração. É neste quadro que se compreende, por exemplo, o regime da falta e vícios da vontade (artigo 240.º e ss. do Código Civil)[148],

[146] Sobre a formação dos contratos em análise no presente trabalho, cf. algumas notas em Matilde Lopes Bettencourt, "A proteção do consumidor...", *ob. cit.*, p. 436. Para aprofundamento sobre a formação contratual, cf. Carlos Ferreira de Almeida, *Contratos,* vol. I, *ob. cit.*, p. 107 e ss.

[147] Axel Metzger, "A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services", *ob. cit.*, pp. 30-33, aborda o modelo de formação dos contratos em análise no presente neste trabalho, pegando em alguns exemplos concretos (*Facebook*, *WhatsApp*, *Spotify* e *Google*), que interpreta como podendo ser percecionados, por um consumidor razoável, como propostas contratuais.

[148] Mafalda Miranda Barbosa, num exemplo apenas entre a vasta doutrina civilística, ensina, de um modo sistematizado e claro, o regime dos vícios da vontade. Cf. Mafalda Miranda Barbosa, *Falta e Vícios da Vontade – Dogmática e jurisprudência em diálogo,*

dos negócios usurários (artigos 282.º a 284.º do Código Civil)[149] e, de um modo geral, os direitos e deveres especiais de informação e esclarecimento pré-contratual do consumidor, enquanto parte débil, previstos em legislação avulsa, como a Lei de Defesa do Consumidor, o Regime dos Contratos à Distância e o Regime das Cláusulas Contratuais Gerais.

Por outro lado, a vontade das partes, mesmo que perfeitamente formada e expressa, não pode conduzir à fixação de um objeto que não seja admitido por lei (280.º e 294.º do Código Civil). No âmbito de contratos de consumo, avultam limitações ao objeto contratual mais apertadas do que as oferecidas pela lei geral, não podendo ser subvertidos, por exemplo, os direitos e garantias do consumidor consagrados, designadamente, nos diplomas acima referidos (entre outros, artigo 16.º da Lei de Defesa do Consumidor e artigo 51.º, n.º 1, do Decreto-Lei n.º 84/2021, de 18 de outubro).

Todas estas normas jurídicas compõem, na sua respetiva medida, os alicerces da formação de um contrato que, por um lado, reflita uma verdadeira e bem formada vontade das partes ao momento da sua celebração, ponderada à luz do diferencial económico de cada uma delas por referência à outra, e que, por outro, garanta no seu objeto, positiva e negativamente, a proteção contratual que o consumidor, de mote próprio, não teve armas para adicionar ao perímetro contratual. Assim, a união das vontades das partes, se formada de acordo com a lei, ditará aquela que constituirá a *justiça interna* do concreto negócio[150]-[151]. Caso em causa esteja um contrato sinalagmático, desta justiça interna decorrerá a justiça do próprio sinalagma, bem como a preparação das partes para assumir o compromisso estabelecido naquele negócio, obrigando-se estas a cumpri-lo nos seus precisos termos.

Iremos, por isso, tecer algumas considerações quanto à adequação da atual legislação de proteção do consumidor, sobretudo em matéria de tutela do esclarecimento pré-contratual e liberdade da manifestação da vontade, para assegurar um efetivo esclarecimento do consumidor e a inerente justiça interna do contrato.

1.ª ed., Coimbra, Gestlegal, 2020, e Mafalda Miranda Barbosa, *Lições de Teoria Geral do Direito Civil*, 1.ª ed., Coimbra, Gestlegal, 2021, pp. 708-820.

149 Para uma análise aprofundada sobre a figura do negócio usurário, cf. Pedro Eiró, *Do Negócio Usurário*, Coimbra, Almedina, 1990.

150 A discussão sobre os critérios de determinação da justiça interna do contrato é longa e complexa (complexidade essa agravada, de resto, perante a atipicidade contratual), conhecendo várias posições que foram sintetizadas em Pedro Pais de Vasconcelos, *Contratos atípicos*, 2.ª ed., Coimbra, Almedina, 2009, pp. 417 e ss.

151 Menezes Leitão, *Direito das Obrigações*, vol. I, *ob. cit.*, p. 24, recorda, a este respeito, as afirmações de Immanuel Kant, segundo o qual "*quando alguém decide alguma coisa por outrem é possível que cometa uma injustiça, mas nenhuma injustiça é possível quando se decide por si próprio*", e de Fouillée, de que "*toda a justiça é contratual, quem diz contratual diz justo*".

5.1 AS OBRIGAÇÕES PRÉ-CONTRATUAIS DE INFORMAÇÃO, *MAXIME* SOBRE PREÇOS

Em acréscimo ao direito geral de informação previsto no artigo 7.º da Lei de Defesa do Consumidor, o seu artigo 8.º, n.º 1, atribui ao consumidor o direito geral "particular" à informação[152] "*clara, objetiva e adequada*" sobre os termos da relação de consumo em que é parte. Correspetivamente a este direito do consumidor, impende sobre profissional o ónus de, tanto na fase de negociações como na fase de celebração de um contrato, informar o consumidor, "*nomeadamente*"[153] sobre as características principais dos bens ou serviços, tendo em conta o suporte utilizado para o efeito e considerando os bens ou serviços em causa, e sobre o "*preço total dos bens ou serviços, incluindo os montantes das taxas e impostos, os encargos suplementares de transporte e as despesas de entrega e postais, quando for o caso*" [154], o "*modo de cálculo do preço, nos casos em que, devido à natureza do bem ou serviço, o preço não puder ser calculado antes da celebração do contrato*", as "*modalidades de pagamento*" e "*as consequências do não pagamento do preço do bem ou serviço*".

Por seu turno, o Regime das Práticas Comerciais Desleais, que é aplicável à generalidade das relações de consumo[155], classifica essas informações como *substanciais*, e essenciais para a decisão do consumidor médio[156], em caso de proposta contratual ou de convite a contratar (artigo 10.º, n.º 1, als. a), c) e d)), cuja omissão se terá por enganosa, nos termos e para os efeitos do artigo 9.º, n.º 1, do mesmo diploma, e que poderá motivar, entre outras sanções, a resolução (artigo 8.º, n.º 4, da Lei de Defesa do Consumidor) ou a anulação do negócio por parte do consumidor (artigo 14.º, n.º 1, do Regime das Práticas Comerciais Desleais).

O Regime dos Contratos à Distância espelha estes normativos no que concerne especificamente aos contratos celebrados à distância e aos contratos celebrados fora do estabelecimento comercial (entre outras, als. d), e) e f) do n.º 1 do artigo 4.º), diploma que, como já vimos, se aplica aos

---

152 Conforme recorda Jorge Morais Carvalho, *Manual de Direito do Consumo*, 7.ª ed. reimp., Coimbra, Almedina, 2021, p. 94, nota 251, o direito à informação do consumidor tem natureza constitucional (artigo 60.º, n.º 1 da Constituição da República Portuguesa).

153 O elenco de itens de informação oferecido por esta norma parece ser meramente indicativo, o que deixa ao intérprete alguma margem para, dentro do mesmo espírito, adaptar o seu conteúdo.

154 Sem aplicação nos contratos sujeitos ao presente trabalho (tão-só aos bens destinados à venda a retalho), mas com valor ilustrativo sobre o modo como o ordenamento jurídico nacional tutela a prestação de informação sobre preços, cf. Decreto-Lei n.º 138/90, de 26 de Abril. A este respeito, Jorge Morais Carvalho, *Manual de Direito do Consumo*, *ob. cit.*, pp. 96-97.

155 Cf. Jorge Morais Carvalho, *Manual de Direito do Consumo*, *ob. cit.*, p. 140.

156 Aquele consumidor "*normal, com um nível de informação mediano e que utiliza uma diligência regular nos contratos que celebra, não relevando o consumidor com nível de informação baixo ou que seja pouco diligente nos seus negócios*". Cf. Jorge Morais Carvalho, *Manual de Direito do Consumo*, *ob. cit.*, p. 144.

contratos que tenham dados pessoais como contraprestação (artigo 2.º, n.º 2, na redação que lhe foi dada pelo Decreto-Lei n.º 109-G/2021, de 10 de dezembro)[157]. Porque *substanciais*, a não prestação destas informações considera-se uma omissão enganosa, para efeitos do Regime das Práticas Comerciais Desleais, nos termos do seu artigo 9.º, n.º 4, al. d) (na redação dada pelo Decreto-Lei n.º 109-G/2021, de 10 de dezembro), aplicando-se o regime geral acima referido.

O objetivo da lei é, compreende-se, garantir que a declaração negocial do profissional tenha um conteúdo mínimo, suficiente e capaz de munir o consumidor da informação necessária a um exercício efetivo de reflexão e ponderação sobre se pretende, de facto, celebrar aquele contrato e assumir as obrigações dele inerentes. Assim, e acompanhando Jorge Morais Carvalho[158], "*quando o artigo 8.º, n.º 1* [da Lei de Defesa do Consumidor] *se refere à informação sobre as características ou o preço do bem ou do serviço, está a impor que da declaração contratual do profissional constem esses elementos, acrescentando como é que estes elementos devem ser incluídos na mensagem emitida*". Assim, continua o autor, "*o profissional encontra-se vinculado a fornecer ao consumidor todos os elementos de que disponha sobre o bem ou o contrato a celebrar (...) que possam ser relevantes para a decisão de contratar. Esta regra resulta quer* [da Lei de Defesa do Consumidor], *quer* [do Regime das Práticas Comerciais Desleais]".

Ora, não obstante a aplicação destes deveres a contratos de consumo sobre fornecimento e conteúdos digitais que caibam no escopo do Decreto-Lei n.º 84/2021, de 18 de outubro, e da Diretiva 2019/770, não cremos que os mesmos estejam adaptados aos casos em que não exista o pagamento de um *preço*. Aliás, não cremos ter sido feliz o legislador no Decreto-Lei n.º 109-G/2021, de 10 de dezembro, que, tendo expressamente introduzido estes contratos no âmbito de aplicação do Regime dos Contratos à Distância, e tendo atualizado o regime das omissões enganosas previsto no Regime das Práticas Comerciais Desleais, no sentido de cobrir o âmbito de aplicação daquele, não procedeu a qualquer adaptação do elenco de informação pré-contratual no sentido de atender às especificidades dos contratos que tenham dados pessoais como contraprestação[159], designadamente quanto

---

157 Para uma análise do Regime dos Contratos à Distância, e comentário sobre o seu contributo no esclarecimento pré-contratual do consumidor (pese embora anterior às alterações introduzidas pelo Decreto-Lei n.º 109-G/2021, de 10 de dezembro), cf. Jorge Morais Carvalho, João Pedro Pinto Ferreira, *Contratos Celebrados à Distância e Fora do Estabelecimento Comercial – Anotação ao Decreto-Lei n.º 24/2014, de 14 de fevereiro*, Coimbra, Almedina, 2014, *maxime* pp. 51 e ss.

158 Cf. Jorge Morais Carvalho, *Manual de Direito do Consumo*, *ob. cit.*, pp. 161-162.

159 Do prisma da proteção de dados, a AEPD alertou também para o facto de a contraprestação sob a forma de fornecimento de dados pessoais impor preocupações diferentes em comparação com os casos em que existe o pagamento de um preço. Diz essa entidade que "*the link made by the Proposal between paying a price with money, and actively giving data as a counter-performance is misleading. While the consumer is aware of what he is*

ao modo e termos do tratamento desses dados pessoais e à riqueza que os mesmos gerarão para o profissional[160].

Não negamos a possibilidade de estas normas, sobretudo as que se reportam às informações pré-contratuais em matéria de preços, serem aplicadas analogicamente no sentido de abarcar a obrigação de prestação dessas informações pré-contratuais[161], porventura em articulação com as obrigações de informação ínsitas no artigo 13.º do RGPD. Essa solução, em qualquer caso, não abona em favor de uma certa e segura aplicação da lei, pelo que se imporia um reforço expresso e claro das obrigações de informação pré-contratual impendentes sobre os profissionais que recorram a este tipo de negócios[162]. Só assim se garantiria um efetivo esclarecimento do consumidor, capaz de formar um contrato intrinsecamente justo[163].

giving when he pays with money, the same cannot be said about data. Standard contractual terms and privacy policies do not make it easy for the consumer to understand what is precisely made with the data collected about him/her. In this context, it has already been debated whether the organisations could be required to reveal more about their decision making in data processing operations, for example about their intention to create value with the data. It can be observed that privacy policies typically contain vague and elastic terms for the description of the use of the data collected, like "improving consumers' experience". Issues of transparency and fairness in terms and conditions of several online services have been raised through some national investigations into social media and other online services". Cf. European Data Protection Supervisor, *Opinion 4/2017…, ob. cit.,* §26, p. 9.

160 De resto, Philipp Hacker, "Regulating the Economic Impact of Data as Counter-Performance...", *ob. cit.*, pp. 62-63, já chamou à atenção para a falta de esclarecimento dos consumidores e titulares de dados pessoais, que tendem a ignorar as políticas de privacidade que lhes são apresentadas, quanto ao modo como os seus dados são tratados. As preocupações geradas por esta falta de conhecimento transcendem a matéria estrita de proteção de dados pessoais, assolando igualmente a formação dos contratos que compreendam no seu objeto o fornecimento de dados pessoais.

161 Hipótese que admitimos por mero exercício académico e em benefício deste trabalho. Não tomamos posição quanto à admissibilidade e limites desta aplicação analógica, cuja viabilidade não é aqui ponderada. Em qualquer caso, Philipp Hacker, "Regulating the Economic Impact of Data as Counter-Performance...", *ob. cit.*, pp. 67-68 pronunciou-se no sentido de que os conceitos de conceitos de "preço e remuneração" e "objeto principal do contrato" presentes no artigo 4.º, n.º 2 da Diretiva 93/13/CEE sejam interpretados restritivamente, sujeitando ao escrutínio e controlo enquanto *abusivas* as cláusulas contratuais que disponham sobre o fornecimento de dados para efeitos de contraprestação.

162 No mesmo sentido, Mafalda Miranda Barbosa, "Negócios onerosos e gratuitos...", *ob. cit*., p. 1850.

163 De resto, a Comissão Nacional de Proteção de Dados, *Parecer/2021/150*, *ob. cit*., p. 2, salienta também que "*os dados pessoais recolhidos e inferidos, aparentemente com base em cláusulas contratuais que a generalidade dos subscritores não tem consciência de ter acordado, também porque na generalidade dos casos a informação relativa ao tratamento de dados pessoais vem apresentada aos consumidores de uma forma muito incompleta ou obscura, não permitindo ao comum cidadão compreender o alcance do mesmo e as consequências para os seus direitos fundamentais*".

5.2 OS DEVERES DE TRANSPARÊNCIA IMPOSTOS PELO REGIME DAS CLÁUSULAS CONTRATUAIS GERAIS

Importa agora uma referência específica ao Regime das Cláusulas Contratuais Gerais, e à Diretiva 93/13/CEE, do Conselho, de 5 de abril de 1993[164], atinente às cláusulas abusivas nos contratos celebrados com os consumidores, em vigor nosso ordenamento jurídico através do referido regime. Esta referência impõe-se dada a expressão da contratação *standardizada* e a sua relevância estatística na celebração de contratos de consumo[165].

Com efeito, em certos casos, ao consumidor poderá não assistir qualquer liberdade de estipulação do conteúdo dos contratos de consumo que pretenda celebrar. Ao invés, ao consumidor serão apresentadas, pelo *predisponente*[166], as condições comerciais unilateralmente fixadas e inegociáveis da relação de consumo a celebrar, em benefício da célere e massificada contratação[167], sob a forma de cláusulas contratuais gerais ou, de um modo genérico, de cláusulas cujo conteúdo é insuscetível de influência por parte do destinatário (artigo 1.º, n.ºs 1 e 2, do Regime das Cláusulas Contratuais Gerais). Nesse contexto, um respeito acrítico por parte da lei quanto à igualdade formal das partes contratuais poderia conduzir à celebração de negócios, não só não compreendidos (e, portanto, não verdadeira e plenamente aceites) pela parte mais débil, mas também contendo condições contratuais que,

---

164 Para uma comparação entre o diploma nacional e o europeu, cf. Jorge Morais Carvalho, *Manual de Direito do Consumo*, *ob. cit.*, p. 121. Para uma anotação ao Regime das Cláusulas Contratuais Gerais, cf. Ana Prata, *Contratos de Adesão e Cláusulas Contratuais Gerais*, 2.ª ed., Coimbra, Almedina, 2021.

165 Cf. Jorge Morais Carvalho, *Manual de Direito do Consumo*, *ob. cit.*, pp. 121-122. A este respeito, note-se que o Comité Europeu de Proteção de Dados, *Diretrizes 2/2019...*, *ob. cit.*, §16, p. 7, reconheceu também que os "*contratos de serviços em linha*", não são, normalmente, individualmente negociados, o que coloca em perigo os princípios da limitação das finalidades e da minimização dos dados. "*Os avanços tecnológicos permitem que os responsáveis pelo tratamento recolham e tratem facilmente mais dados pessoais do que nunca. Consequentemente, existe um risco grave de os responsáveis pelo tratamento poderem procurar incluir cláusulas gerais de tratamento nos contratos, a fim de maximizar a possível recolha e utilização de dados, sem especificarem adequadamente as finalidades ou ponderarem a possibilidade de impor obrigações de minimização dos dados*".

166 Conforme ensina Carlos Ferreira de Almeida, *Contratos,* vol. I, *ob. cit.*, pp. 186 e ss., ao predisponente, enquanto a parte que propõe as cláusulas contratuais gerais, opõe-se o aderente, que a elas adere. Em tese, qualquer uma destas figuras pode assumir qualquer uma das três posições típicas do processo contratual tal como previsto no Código Civil - a de proponente, destinatário da proposta ou aceitante -, dependendo, *in casu*, de se a disponibilização das cláusulas contratuais gerais constitui uma proposta contratual, um convite a contratar ou a aceitação. Cf. também Jorge Morais Carvalho, *Manual de Direito do Consumo*, *ob. cit.*, p. 91.

167 Para uma maior elaboração acerca do papel desempenhado pelas cláusulas contratuais gerais no comércio, os seus usos e os seus perigos *vide*, por exemplo, Menezes Cordeiro, *Tratado de Direito Civil*, vol. II, *ob. cit.*, pp. 363 e ss. ou Carlos Ferreira de Almeida, *Contratos,* vol. I, *ob. cit.*, pp. 179 e ss.

mesmo que devidamente compreendidas, poderiam desencadear relações contratuais injustas, abusivas, desequilibradas, que apenas foram aceites em virtude do débil (ou ausente) poder negocial da parte aderente[168-169].

Perante este circunstancialismo, o legislador fez impender sobre os predisponentes um ónus de comunicação e um dever de informação (artigos 5.º e ss. do Regime das Cláusulas Contratuais Gerais), cuja violação é cominada com a exclusão das cláusulas em causa dos contratos (artigo 8.º do Regime das Cláusulas Contratuais Gerais, que opera a mesma exclusão quanto a cláusulas que, por razões gráficas, passem despercebidas a um contratante normal, bem como a cláusulas inseridas em formulários depois destes terem sido assinados por algum dos contratantes)[170]. Assim, nos termos do artigo 5.º, n.ºs 1 e 2, ao predisponente assiste o ónus de comunicar integral, oportuna e adequadamente as cláusulas contratuais gerais aos aderentes, "*para que, tendo em conta a importância do contrato e a extensão e complexidade das cláusulas, se torne possível o seu conhecimento completo e efectivo por quem use de comum diligência*". Adicionalmente, o artigo 6.º impõe ao contratante que recorra a cláusulas contratuais gerais o dever de "*informar, de acordo com as circunstâncias, a outra parte dos*

168 As cláusulas contratuais gerais, antes da entrada em vigor do Regime das Cláusulas Contratuais Gerais ficavam sujeitos à disciplina geral do Código Civil, que, em qualquer caso, mitigava já alguns destes riscos, através da ação das normas sobre a perfeição da declaração negocial (224.º e ss. do Código Civil), sobre os limites do objeto negocial (artigo 280.º do Código Civil) ou sobre a celebração de negócios usurários (artigos 282.º a 284.º do Código Civil). Cf. Ribeiro de Faria, *Direito das Obrigações*, *ob. cit.*, p. 228.

169 Este binómio de preocupações (*proteção da vontade* e *controlo do objeto negocial*) foi igualmente identificado por Almeida Costa como presidindo ao desenho do Regime das Cláusulas Contratuais Gerais. Cf. Almeida Costa, *Direito das Obrigações*, *ob. cit.*, p. 247. Para uma análise aprofundada sobre o défice de autodeterminação do aderente, cf. Joaquim de Sousa Ribeiro, *O Problema do Contrato...*, *ob. cit.,* pp. 275 e ss. e pp. 323 e ss.

170 Não é pacífica a natureza jurídica da cominação de "exclusão" das cláusulas não comunicadas e/ou informadas do contrato, constante do artigo 8.º do Regime das Cláusulas Contratuais Gerais. Com efeito, Ana Prata, *Contratos de Adesão...*, *ob. cit.*, pp. 297 e ss., nota que a distinção entre uma tal consequência e a nulidade poderá não se justificar, dando nota da divergência doutrinal sobre este tema. Assumimos a posição de que as cláusulas não comunicadas e/ou informadas devem considerar-se inexistentes, e não meramente inválidas, desde logo porque tal parece ter sido a intenção deliberada do legislador, que, no mesmo diploma, previu a nulidade como cominação para outras situações. De resto, a nosso ver, a circunstância de a lei cominar a não comunicação e/ou informação com uma sanção tão severa como sua exclusão desse clausulado do perímetro contratual revela a notória preocupação do Regime das Cláusulas Contratuais Gerais em, mais ainda do que a delimitar um certo âmbito de *moralidade contratual* dentro do qual o predisponente poderá desenhar o clausulado, *garantir a ciência do aderente* relativamente aos termos contratuais a que se estará a vincular e a obrigar a cumprir, num papel afim àquele desempenhado pela obrigação de proceder segundo as regras da boa-fé na fase negocial e pré-negocial (artigo 227.º, n.º 1 do Código Civil). Sobre o papel da *culpa in contrahendo* no seio da proteção do contraente débil, *vide* Menezes Cordeiro, *Tratado de Direito Civil*, vol. II, *ob. cit.*, pp. 223 e ss.

aspectos nelas compreendidos cuja aclaração se justifique", bem como de prestar "*todos os esclarecimentos razoáveis solicitados*".

Este regime reforça e complementa aquele oferecido pelos deveres de informação pré-contratual aplicáveis pelos demais diplomas de proteção do consumidor, designadamente a Lei de Defesa do Consumidor, o Regime das Práticas Comerciais Desleais e o Regime dos Contratos à Distância. Com efeito, se a aplicação destes se materializa, na prática e como vimos, na definição do *âmbito mínimo do clausulado* dos contratos de consumo sob o seu âmbito (designadamente de fornecimento de conteúdos e serviços digitais), as referidas normas do Regime das Cláusulas Contratuais Gerais, atribuem ao consumidor uma segunda camada de proteção para os casos em que aquele não possa influenciar as condições comerciais da prestação.

Ora, o Regime das Cláusulas Contratuais Gerais, sendo hoje um diploma basilar no direito das obrigações português, introduziu no nosso ordenamento jurídico o corpo de normas especiais que o legislador entendeu adequado a mitigar os impactos da ausência de liberdade de estipulação e negociação, e da qual resultaria a formação de um clausulado justo e moldado à vontade de cada parte. O método adotado pelo legislador visou, assim, erigir uma certa igualdade *material* das partes contratantes, ao obrigar o predisponente, preventivamente à celebração do negócio, a especiais deveres de transparência. No quadro de uma relação de consumo, estes deveres de transparência edificam-se em órbita daqueles propostos pela legislação já referida.

6. CONCLUSÕES

Perante tudo o que aqui expusemos, é nossa opinião que o artigo 6.º, n.º 1, al. b), do RGPD não se opõe à ideia de que a própria dinâmica, lógica e equilíbrio internos do contrato possa justificar que o tratamento de dados pessoais fornecidos como contraprestação seja considerado como necessário à execução do mesmo. Todavia, a exequibilidade dessa hipótese depende sempre da boa formação e compreensão do negócio, pelas suas partes, *maxime* pelo consumidor/titular dos dados pessoais.

De facto, no âmbito da formação de uma relação de consumo, a fragilidade da posição do consumidor é contrabalançada pela promoção do seu esclarecimento, posição à qual o direito do consumo dedica uma ampla proteção. Para fazer face à impossibilidade de adaptar o clausulado contratual às específicas necessidades e preferências do consumidor, a aposta do legislador recaiu sobre dois vetores.

Por um lado, *ao nível pré-contratual*, o legislador procurou garantir a efetiva tutela da formação da vontade negocial do consumidor, quer através dos deveres de informação pré-contratual lançados pela legislação de pro-

teção do consumidor *strictu sensu*, quer ainda pelos aplicáveis pelo Regime das Cláusulas Contratuais Gerais.

Por outro lado, *ao nível contratual*, o legislador visou os termos da própria relação de consumo, ao atribuir ao consumidor, positivamente, determinados direitos subjetivos sobre o profissional, desde logo atinentes à qualidade dos bens e serviços (artigo 4.º da Lei de Defesa do Consumidor, e Decreto-Lei n.º 84/2021, de 18 de outubro), e expurgando do contrato as cláusulas contratuais gerais que, porque injustas ou abusivas, se devam ter por proibidas, nos termos do Regime das Cláusulas Contratuais Gerais (naturalmente, sem prejuízo da aplicação dos regimes gerais previstos no Código Civil, designadamente em matéria de negócios usurários).

Aplicando-se estas limitações a qualquer profissional operante no mercado livre, a lei confia, a partir daí, que o consumidor encontrará nele uma oferta que se adeque às suas necessidades e exigências, devendo, nessa medida, ficcionar-se o contrato de consumo em causa como justo – retomando as partes, de algum modo, o seu equilíbrio, assente no princípio da igualdade material, uma vez celebrado o contrato. Assim, ambas ficarão sujeitas ao princípio do *pacta sunt servanda* nos termos gerais, que operará com a mesmo extensão e regime reconhecido a um qualquer contrato sinalagmático.

Esta ficção, porém, não poderá ocorrer, sem mais, num cenário em que as limitações acima referidas não sejam verdadeiramente operantes, o que entendemos ser o caso nos contratos que tenham o fornecimento de dados pessoais como contraprestação. Com efeito, a lei, no plano pré-contratual, não oferece garantias de esclarecimento do consumidor quanto aos termos da sua contraprestação nesses casos: salvo a possibilidade, com as fragilidades de segurança e certeza jurídica inerentes, de aplicação analógica de normas já em vigor em matéria de preços, não é exigível ao profissional informar contratualmente o consumidor sobre o valor dos seus dados pessoais, os termos em que os mesmos serão tratados para efeitos da sua monetização (partindo já das obrigações de informação impostas pelo artigo 13.º do RGPD[171] e em respeito dos demais princípios previstos no RGPD aplicáveis) e a riqueza que será gerada.

A lei não garante, assim, os meios para uma compreensão panorâmica dessa relação de consumo por parte do consumidor, promovendo a perce-

[171] É importante aqui dar nota de que o RGPD não obriga a que o elenco de informações devidas ao abrigo do artigo 13.º constitua parte do clausulado contratual. Em qualquer caso, a prestação de todo o elenco de informações devido ao abrigo do artigo 13.º do RGPD, porque desenhado numa perspetiva de proteção de dados pessoais, não está talhado para assegurar o esclarecimento pré-contratual do consumidor (mas tão-só do titular dos dados pessoais), designadamente quanto à ciência da celebração de um contrato sinalagmático e oneroso, e em que os seus dados pessoais funcionarão como contraprestação. Por exemplo, o artigo 13.º não impõe que o titular dos dados pessoais seja esclarecido quanto ao valor económico dos seus dados pessoais nem quanto à riqueza que o seu tratamento gerará.

ção de gratuitidade e unilateralidade das mesmas, uma vez que a lei não prevê obrigações de informação pré-contratual direcionadas para o esclarecimento do consumidor/titular dos dados, no sentido de lhe revelar a "não gratuitidade" do contrato. Com efeito, não estando garantida a informação necessária para que o titular dos dados tome uma decisão e formule uma declaração negocial plenamente esclarecida quanto ao modo como os dados pessoais fornecidos como contraprestação contribuirão para a compensação do profissional pelos conteúdos ou serviços fornecidos, revela-se complexo demonstrar o nexo entre a execução do contrato e o tratamento dos dados pessoais, por referência ao *objeto fundamental* e lógica a si subjacentes (e, bem assim, a ciência do titular dos dados quanto aos mesmos), em linha com as orientações do CEPD.

Esta insuficiência de regime ao nível do esclarecimento pré-contratual do consumidor irá, a jusante, coartar também o controlo promovido em sede de regulação de cláusulas contratuais gerais. Com efeito, no seu estado atual, a lei permite predispor cláusulas contratuais gerais com um certo minimalismo em matéria de contraprestação do consumidor, sem que com isso se incumpra, necessariamente, o ónus da comunicação e o dever de informação previstos nos artigos 5.º e ss. do Regime das Cláusulas Contratuais Gerais. Em decorrência, permite-se também ao predisponente limitar a exposição ao risco de as cláusulas contratuais gerais predispostas serem consideradas excluídas do contrato, bem como o risco de invalidade total do mesmo (artigo 8.º, als. a) e b) e artigo 9.º, n.º 2, do mesmo diploma).

Assim, a adequação do fundamento de licitude em análise — sendo certo que sempre dependeria de uma avaliação caso a caso —, num cenário em que a lei não oferece hoje garantias (melhor, indícios) de que o consumidor compreende globalmente o objeto e dinâmica fundamentais dos "negócios gratuitos" que celebra, não pode ser, nem em exercício académico, confortavelmente assumida. Com efeito, se do ponto de vista estrito de direito da proteção de dados pessoais cremos que o fundamento de licitude previsto no artigo 6.º, n.º 1, al. b), do RGPD oferece latitude suficiente para cobrir as operações de tratamento de dados pessoais necessários ao ressarcimento do profissional (pese embora, tradicionalmente, a necessidade para a execução do contrato tenha vindo a ser interpretada num sentido *operacional*), o direito do consumidor não estabelece, como devia, os alicerces sobre os quais os consumidores formariam uma vontade esclarecida de contratar naqueles moldes. Na criação de um regime jurídico próprio para os contratos que prevejam o fornecimento de dados pessoais como contraprestação, o legislador (comunitário e nacional) pecou por defeito, não tendo atingido a amplitude de regime que devia. Foi, numa palavra, o seu pior inimigo, já que o caminho que ficou por percorrer era precisamente aquele que, no nosso ver, asseguraria a plena compatibilidade deste modelo de negócio com o direito da proteção de dados pessoais, e permitiria ultrapassar, sem detrimen-

to das garantias e proteção do consumidor/titular dos dados, a exigência da prestação do seu consentimento.

A lei não assegura, em suma, um grau mínimo de compreensão por parte do consumidor sobre o funcionamento do negócio num todo, com as especificidades atinentes ao facto de pressupor o fornecimento de dados pessoais (e o seu tratamento) como contraprestação, o que influirá negativamente na sustentação do recurso à necessidade (económica) para execução do contrato, com recurso à fundamentação cujas traves-mestras ensaiamos no presente trabalho.

7. BIBLIOGRAFIA

Almeida, Carlos Ferreira de - *Contratos,* vol. I, 7.ª ed., Coimbra, Almedina, 2022. ISBN: 9789894000914.

Barbosa, Mafalda Miranda – "Negócios onerosos e gratuitos: uma reflexão a propósito de novos fenómenos de gratuitidade"*, in* Revista de Direito Comercial (2020), publicação *online*, disponível em https://www.revistadedireitocomercial.com/negocios-onerosos-e-gratuitos (12.01.2022).

Barbosa, Mafalda Miranda – *Falta e Vícios da Vontade – Dogmática e jurisprudência em diálogo,* 1.ª ed., Coimbra, Gestlegal, 2020. ISBN: 978-989-8951-32-8.

Barbosa, Mafalda Miranda – *Lições de Teoria Geral do Direito Civil,* 1.ª ed., Coimbra, Gestlegal, 2021. ISBN: 978-989-8951-57-1.

Bettencourt, Matilde Lopes de Mendonc a Ortins de – "A protec ão do consumidor em contratos digitais: análise dos contratos celebrados com dados pessoais como contraprestac ão", *in Anuário do NOVA Consumer Lab*, publicação *online*, Ano 3 (2021), pp. 387–476, disponível em http://novaconsumerlab.novalaw.unl.pt/wp-content/uploads/2022/02/NOVA-Consumer-Lab-2021.pdf (20.03.2022). ISSN: 2184-6200

Carneiro, Patrícia Filipa Pereira - "*Coisificação" dos dados pessoais no âmbito das relações contratuais*, FDUP, 2019. Dissertação de mestrado.

Carvalho, Jorge Morais - *Compra e Venda e Fornecimento de Conteúdos e Serviços Digitais – Anotação ao Decreto-Lei n.º 84/2021, de 18 de outubro*, Coimbra, Almedina, 2022. ISBN: 978-989-40-0183-6.

Carvalho, Jorge Morais – *Manual de Direito do Consumo*, 7.ª ed. reimp., Coimbra, Almedina, 2021. ISBN: 9789724083407

Carvalho, Jorge Morais, FERREIRA, João Pedro Pinto – *Contratos Celebrados à Distância e Fora do Estabelecimento Comercial – Anotação ao Decreto-Lei n.º 24/2014, de 14 de fevereiro*, Coimbra, Almedina, 2014. ISBN: 978-972-40-5650-0.

Carvalho, Orlando (*aut.*), Fernandes, Francisco Liberal, Guimarães, Maria Raquel, Redinha, Maria Regina (*coords.*) – *Teoria Geral do Direito Civil*, 4.ª ed., Coimbra, Gestlegal, 2021. ISBN: 978-989-8951-74-8.

Coelho, Francisco Manuel de Brito Pereira – *Contratos Complexos e Complexos Contratuais*, 1.ª ed., Coimbra, Coimbra Editora, 2014. ISBN 9789723222555.

Comissão Nacional de Proteção de Dados, *Parecer/2021/100*, Lisboa, adotado em 22 de julho de 2021.

Comissão Nacional de Proteção de Dados - *Parecer/2021/150*, Lisboa, adotado em 23 de novembro de 2021.

Comité Europeu de Proteção de Dados - *Diretrizes 2/2019 sobre o tratamento de dados pessoais ao abrigo do artigo 6.º, n.º 1, alínea b), do RGPD no contexto da prestação de serviços em linha aos titulares dos dados*, adotadas em 8 de outubro de 2019.

Comité Europeu de Proteção de Dados, *Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679*, adotadas em 4 de maio de 2020.

Cordeiro, A. Barreto Menezes – *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, 2021. ISBN: 9789724092614.

Cordeiro, António Menezes – *Código Civil Comentado I – Parte Geral*, Coimbra, Almedina, 2020. ISBN 978-972-40-8453-4.

Cordeiro, António Menezes – *Tratado de Direito Civil*, vol. I, 4.ª ed. reimp., Coimbra, Almedina, 2021. ISBN 9789724047768.

Cordeiro, António Menezes – *Tratado de Direito Civil*, vol. II, 5.ª ed., Coimbra, Almedina, 2021. ISBN 9789724091860.

Costa, Inês Silva – "A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas", *in Revista Electrónica de Direito* (RED), publicação *online*, ISSN: 21829845, Vol. 24, n.º 1 (2021), pp. 33-82, disponível em https://cije.up.pt//client/files/0000000001/4-ines-costa_1677.pdf (12.06.2022).

Costa, Mário Júlio de Almeida – *Direito das Obrigações*, 12.ª ed. reimp., Coimbra, Almedina, 2020. ISBN: 9789724040332

Duarte, Rui Pinto – *Tipicidade a Aticipidade dos Contratos*, Coimbra, Almedina, 2000.

Eiró, Pedro – *Do Negócio Usurário*, Coimbra, Almedina, 1990. ISBN: 972-40-0468-6.

European Data Protection Supervisor - *Opinion 4/2017, on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, adotada em 14 de março de 2017.

European Data Protection Supervisor - *Opinion 8/2016 - EDPS Opinion on coherent enforcement of fundamental rights in the age of big data,* adotada em 23 de setembro de 2016.

Faria, Jorge Ribeiro de – *Direito das Obrigações*, vol. I, 2.ª ed., Coimbra, Almedina, 2020. ISBN 9789724086538.

Fries, Martin – "Data as Counter-Performance in B2B Contracts", *in* Lohsse, Sebastian; Schulze, Reiner; Staudenmayer, Dirk (*eds. lits.*), *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 253-261. ISBN: 978-1-5099-4031-8.

Gisclard, Thibault – "Limitations of Autonomy of the Will in Conventions of Exploitation of Personality Rights", *in International Review of Intellectual Property and Competition Law* (IIC), Vol. 45, n.º 1 (2014), pp. 18–42, ISSN 0018-9855, 2195-0237.

Grupo de Trabalho do Artigo 29.º - *Documento de Trabalho 02/2013 dando orientac ões sobre a obtenc ão de consentimento para testemunhos de conexão*, adotado em 2 de outubro de 2013.

Grupo de Trabalho do Artigo 29.º - *Parecer 06/2014 do sobre o conceito de interesses legítimos do responsável pelo tratamento na aceção do artigo 7.º da Diretiva 95/46/CE (WP217)*, adotado em 9 de abril de 2014.

Grupo de Trabalho do Artigo 29.º - *Parecer 2/2010 sobre publicidade comportamental em linha*, em 22 de junho de 2010.

Guimarães, Maria Raquel - "A conformação da liberdade contratual pela cláusula geral da ordem pública", *in* LUCÁN, Mª Ángeles Parra (*dir.*); LERA, Silvia Gaspar (*coord.*), *Derecho y autonomía privada: una visión comparada e interdisciplinar*, Granada, Comares, 2017, pp. 413-434. ISBN: 978-84-9045-521-0.

Güven Taştan, Furkan – *The (im)possibility of personal data as an object of contracts: An analysis of the GDPR and the Digital Content Directive*, Tilburg, Universidade de Tilburg, julho 2021 (27.02.2022). Dissertação de Mestrado.

Hacker, Philipp - "Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive", in loHSSE, Sebastian; schulze, Reiner; staudenmayer, Dirk (*eds. lits.)*, *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 47-76. ISBN: 978-1-5099-4031-8.

hermstrüwer, Yoan – "Digital Content and Sales or Service contracts under EU Law and Belgian/French Law", *in Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (JIPITEC), publicação *online*, ISSN: 2190-3387, Vol. 8, n.º 1 (2017), pp. 9–27, disponível em https://www.jipitec.eu/issues/jipitec-8-1-2017 (03.01.2022).

Jacquemin, Hervé – "Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data", *in Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (JIPITEC), publicação *online*, ISSN: 2190-3387, Vol. 8, n.º 1 (2017), pp. 27–38, disponível em https://www.jipitec.eu/issues/jipitec-8-1-2017 (03.01.2022).

Janeček Václav, Malgieri Gianclaudio – "Data Extra Commercium", *in* Lohsse, Sebastian; Schulze, Reiner; Staudenmaier, Dirk (*eds. Lits.)*, *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 95-125. ISBN: 978-1-5099-4031-8.

Kull, Irene - "Withdrawal from the Consent to Process Personal Data Provided as Counter-Performance: Contractual Consequences", *in Journal of the University of Latvia*, Vol. 13 (2020). ISSN: 16917677.

Kuner, Christopher; Bygrave, Lee A.; Docksey, Christopher (eds.) – *The EU General Data Protection Regulation (GDPR): a commentary*, Oxford, Oxford University Press, 2020. ISBN. 9780198826491.

Leitão, Luís Manuel Teles de Menezes – *Direito das Obrigações*, vol. I, 16.ª ed., Coimbra, Almedina, 2022, ISBN 9789894001966.

Lohsse, Sebastian, Schulze, Reiner, Staudenmayer, Dirk – "Data as Counter-Performance – Contract Law 2.0? An Introduction", *in* Lohsse, Sebastian;

Schulze, Reiner; Staudenmayer, Dirk (*eds. lits.)*, *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 9-21. ISBN: 978-1-5099-4031-8.

Metzger, Axel - "Data as Counter-Performance: What Rights and Duties do Parties Have?", *in Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (JIPITEC), Vol. 8, n.º 1 (2017), pp. 2-8, ISSN: 2190-3387, publicação *online* disponível em https://www.jipitec.eu/issues/jipitec-8-1-2017 (03.01.2022)

Metzger, Axel – "A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services", *in* Lohsse, Sebastian; Schulze, Reiner; Staudenmayer, Dirk (*eds. lits.)*, *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 25-45. ISBN: 978-1-5099-4031-8.

Narciso, Madalena - "Dados Pessoais como Contraprestação em Contratos de Consumo – Breve Reflexão"*, in* Carvalho, Jorge Morais (*coord*.); Silva, Maria Miguel Oliveira (*ed.*), *Anuário do NOVA Consumer Lab*, Ano 1 – 2019 (janeiro 2020), pp. 129-147, ISSN: 2184-7185, disponível em http://novaconsumerlab.fd.unl.pt/wp-content/uploads/2020/01/Anuário-NOVA-Consumer-LAB-2019.pdf (01.12.2021)

Pereira, Maria de Lurdes – *Conceito de prestação e destino da contraprestação*, Coimbra, Almedina, 2001. ISBN: 972-40-1527-0.

Pinto, Carlos Alberto Da Mota; Monteiro, António Pinto; Pinto, Paulo Mota – *Teoria Geral do Direito Civil*, 5.ª ed., Coimbra, Gestlegal, 2020, ISBN 978-989-8951-53-3.

Pinto, Paulo Mota – *Direitos de Personalidade e Direitos Fundamentais - Estudos*, 1.ª ed., Coimbra, Gestlegal, 2018, ISBN 978-989-54076-3-7.

Pires, Catarina Monteiro – *Impossibilidade da Prestação*, Coimbra, Almedina, 2020. ISBN 9789724084626.

Prata, Ana – *Contratos de Adesão e Cláusulas Contratuais Gerais*, 2.ª ed., Coimbra, Almedina, 2021. ISBN: 978-972-40-8532-6.

PROENÇA, José Carlos Brandão – "Da «justa medida» (proporcionalidade) no Título I (das obrigações em geral) do Livro II do Código Civil de 1966.*", in Estudos de Direito das Obrigações. Contrato-promessa. Responsabilidade civil. Da proporcionalidade obrigacional,* Porto, Universidade Católica Editora, 2018. ISBN: 9789898835352

Ribeiro, Joaquim de Sousa – *O Problema do Contrato — As Cláusulas Contratuais Gerais e o Princípio da Liberdade Contratual*, Coimbra, Almedina, 1999. ISBN: 9789724011769.

Sattler, Andreas – "Autonomy or Heteronomy – Proposal for a two-tier interpretation of Art. 6 GDPR", *in* Lohsse, Sebastian; Schulze, Reiner; STAUDENMAYER, Dirk (*eds. Lits.)*, *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 225-251. ISBN: 978-1-5099-4031-8.

Schmidt-Kessel, Martin – "Right to Withdrawn Consent to Data Processing – The Effect on the Contract", in Lohsse, Sebastian; Schulze, Reiner; Staudenmayer,

Dirk (*eds. Lits.)*, *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 129-146. ISBN: 978-1-5099-4031-8.

Sein, Karin; Spindler, Gerald – "The new Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1", *in European Review of Contract Law*, Vol. 15, n.º 3 (2019), pp. 257-279. ISSN 1614-9939, 1614-9920.

Sénéchal, Juliette – "Article 16(2) of the 'Digital Content and Digital Services' Directive on the Consequences of Termination of Contract, or the Difficult Articulation between Union Law on Consumer Contract and Union Law on the Protection of Personal Data", *in* Lohsse, Sebastian; Schulze, Reiner; Staudenmayer, Dirk (*eds. Lits.)*, *Data as Counter-Performance – Contract Law 2.0?, 5th Münster Colloquia on EU Law and the Digital Economy V*. Baden-Baden, Nomos/Hart Publishing, 2020, pp. 147-162. ISBN: 978-1-5099-4031-8.

Vasconcelos, Pedro Pais de – *Contratos atípicos*, 2.ª ed., Coimbra, Almeida, 2009, ISBN 9789724037011.

Vasconcelos, Pedro Pais de; Vasconcelos, Pedro Leitão Pais de – *Teoria Geral do Direito Civil*, 9.ª ed. reimp., Coimbra, Almedina, 2022, ISBN 9789724081847.

Versaci, Giuseppe – "Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection", *in European Review of Contract Law*, Vol. 4, n.º 4 (2018), pp. 374–392. ISSN 1614-9939, 1614-9920.

IV

IMPACTO DA TECNOLOGIA E REGULAÇÃO

AUTODETERMINAÇÃO DIGITAL NO CONTEXTO COVID 19

Eduardo Braga Tavares Paes

eduardo@tavarespaes.com.br

Resumo: O presente trabalho tem como objetivo examinar os impactos de algumas das medidas adotadas pelas autoridades públicas no contexto da pandemia do COVID-19, especialmente na União Europeia e mais especificamente em Portugal, relativamente ao conjunto de normas de proteção de dados. A análise é feita partir dos conceitos jurídicos que interessam ao direito da proteção de dados, tendo como norte a autodeterminação informativa digital. O estudo versa sobre temas concretos como o tratamento de dados de saúde pelas autoridades públicas com divulgação de informações sobre infetados, a imposição de obrigação de instalação e operação de aplicação que permite o rastreio de contatos de infetados e, também, a criação e utilização do chamado Certificado Digital COVID-19. O confronto dessas situações com o ordenamento jurídico voltado à proteção de dados pessoais permite conhecer a medida da eficácia dos instrumentos legais de proteção dos dados pessoais de saúde no ambiente da COVID-19.

Palavras-chave: Privacidade, Proteção de Dados, Direitos da Personalidade, Autodeterminação Digital, Regulamento Geral de Proteção de Dados, RGPD, Stayaway Covid, Certificado Digital COVID-19 da UE

Abstract: The present paper proposes an analysis of the impacts of certain measures adopted by public authorities in the context of the COVID-19 pandemic, especially in the European Union and in Portugal, regarding data protection rules. The analysis is based upon legal concepts related to data protection law, guided by digital informational self-determination. This paper explores specific topics such as processing of health data by public authorities regarding disclosure of information about infected people, the obligation to install and operate an application that leads to tracing of contacts of infected people and, also, the creation and operation of COVID-19 Digital Certificates. Examining such situations with regard to data protection law is important for the effectiveness test of statutory provisions for personal data concerning health in COVID-19 environment.

Keywords: Privacy, Data Protection, Personality Rights, Self-determination, General Data Protection Regulation, GDPR, Stayaway Covid e EU Digital COVID-19 Certificate – EUDCC

1. INTRODUÇÃO

Na sua premiada obra intitulada *Ensaio sobre a Cegueira*[1], *José Saramago narra a história de um homem que perde a visão, acometido de uma doença (cegueira branca). A doença transmite-se, em seguida, ao seu médico, a um*

[1] Cf. José Saramago – Ensaio sobre a Cegueira. Lisboa: Livraria Lello e Porto Editora, 2021.

ladrão (que lhe furta o carro) e, assim por diante, se alastra a toda a comunidade. Esse foi o início do que se transformou numa pandemia, combatida pelas autoridades dessa sociedade imaginária com extremo rigor e violência. Uma das consequências da pandemia, segundo Saramago, seria a de desvendar a verdade sobre a sociedade, revelando os seus dramas e paradoxos intrínsecos.

Parece que se trata de uma lógica inegável que Saramago, como bom conhecedor da alma humana, soube extrair da realidade: a propagação de uma doença em grande escala tem a especial aptidão para desorganizar a sociedade e tornar público o que subjaz, escondido, nas suas camadas mais internas, os seus íntimos dilemas.

Quase um quarto de século depois da publicação do livro, já em dezembro de 2019, a Comissão Municipal de Saúde da cidade de Wuhan, a cidade mais importante e populosa da China Central, comunicou ao mundo a ocorrência de 27 casos de pneumonia por síndrome respiratória aguda causada por uma nova variante do Coronavírus (que, posteriormente, se convencionou chamar COVID-19)[2]. Essa nova doença gerava manifestações clínicas severas, diferentes das que se viam nas pneumonias comuns, com um aspeto bastante especial: a resposta aos tratamentos convencionais não era satisfatória e muitos casos conduziam ao óbito. Destacava-se, além da mortalidade acentuada, a preocupante contagiosidade.

Em pouco tempo, o vírus ultrapassou fronteiras e alcançou muitos países, em todos os continentes. A Organização Mundial de Saúde – OMS, em 30 de janeiro de 2020, declarou emergência de saúde pública de âmbito internacional e, a 11 de março de 2020, classificou a situação de saúde como pandemia[3]. No dia seguinte, em Portugal, o Conselho de Ministros se reuniu para expedir um Comunicado com diversas medidas extraordinárias de resposta à pandemia do novo coronavírus.

Sem defesa contra esse novo vírus, a humanidade viu-se diante do que se tornou a maior e mais violenta pandemia dos últimos 100 anos, de consequências económicas, políticas e sociais muito mais terríveis do que aquelas vislumbradas por Saramago.

A realidade e a ficção aproximam-se quando, tal como no flagelo do Ensaio, a pandemia da COVID-19 trouxe, além da insegurança social pelos riscos envolvidos para a saúde pessoal e coletiva, a urgência em se encontrarem solu-

---

[2] A propósito das circunstâncias dessa descoberta, veja-se Clara Barata – "O que aprendemos sobre o covid-19 nos últimos dois anos" *in Jornal Público*, edição de 31.12. 2021. Disponível em https://www.publico.pt/2021/12/31/ciencia/noticia/aprendemos-covid19-ultimos-dois-anos-1990319 19.03. 2022.

[3] A propósito da evolução cronológica da COVID-19, consulte-se "Event Background COVID-19" *in European Center for Disease Prevention and Control Cfr. European Center for Disease Prevention and Control*, Disponível em https://www.ecdc.europa.eu/en/novel-coronavirus/event-background-2019 – Consultado em 21.04. 2022.

ções mágicas para enfrentar a ameaça, sem o cuidado de serem perfeitamente compatíveis com o ordenamento jurídico vigente.

No campo jurídico, destaca-se a repercussão da pandemia nomeadamente em relação a um ponto de interesse que se vinha tornando cada vez mais objeto de preocupação e cuidado dos juristas, especialmente na União Europeia: o da proteção da privacidade dos dados pessoais, que molda e regulamenta as políticas de uso desses dados e que estabelece diretrizes para a segurança e privacidade das informações individuais.

Apesar de todo o arcabouço legal e regulamentar destinado à proteção dos dados pessoais, fundado e reforçado por uma legislação complexa e dotada de instrumentos preciosos à sua operacionalização, os interesses que se consideravam bem protegidos ficaram sob ameaça desde o surgimento da pandemia.

Yuval Noah Harari[4] asseverou, já no início de 2020, no raiar dos novos tempos, que a tempestade passaria, mas as escolhas que se fizessem naquele momento poderiam moldar as nossas vidas no futuro, especialmente aquelas situadas entre a supervisão totalitária e a cidadania fortalecida ou entre o isolamento nacionalista e a solidariedade global.

Preocupava-lhe o risco de que os tempos anormais fossem pretexto para contramedidas extremas pelas autoridades, com o objetivo de permitir ou ampliar o monitoramento da população, por meio da aplicação de técnicas de rastreamento digitais que avançassem sobre conquistas civilizacionais relativas aos direitos à intimidade e às garantias de proteção dos dados dos cidadãos.

Esta ideia foi compartilhada por muitos[5] e naturalmente conduz à indagação inevitável quanto à real efetividade das medidas legislativas, princípios e instrumentos jurídicos concebidas para a proteção dos interesses dos cidadãos num cenário não pandémico, quando postas em causa ante situações extremas tais como as que se impuseram em todos os campos.

---

[4] Cf. Yuval Noah HARARI, "O mundo após o do coronavírus" *in Financial Times, edição online de* 20.01.2020. Disponível em https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 Consultado em 30.02.2022. No texto, o autor destaca, ainda: "*Humankind is now facing a global crisis. Perhaps the biggest crisis of our generation. The decisions people and governments take in the next few weeks will probably shape the world for years to come. They will shape not just our healthcare systems but also our economy, politics and culture. We must act quickly and decisively. We should also take into account the long-term consequences of our actions. When choosing between alternatives, we should ask ourselves not only how to overcome the immediate threat, but also what kind of world we will inhabit once the storm passes. Yes, the storm will pass, humankind will survive, most of us will still be alive — but we will inhabit a different world*".

[5] Cf. Li C. Tiffany – "Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis", *in Chicago Law Journal* 767- *Loyola University*, (2021). Disponível em https://scholars.unh.edu/cgi/viewcontent.cgi?article=1459&context=law_facpub. Consultado em 18.07.2022.

Quando os riscos que a propagação do coronavírus trouxe para a sociedade se agigantaram e diante de toda a incerteza que passou a existir a partir do início do ano de 2020, com a possibilidade de colapso estrutural, medidas extremas, concernentes à utilização de dados pessoais como parte de medidas de impacto empregadas no combate da pandemia, que não eram antes sequer cogitadas, passaram a ser efetivamente consideradas e, em alguns casos, foram aplicadas.

No presente estudo, algumas dessas medidas serão examinadas, com abordagem do conflito de interesses jurídicos que resulta dessa situação, em especial sob o prisma do direito à privacidade e da proteção dos dados sensíveis. Procurar-se-á analisar o conjunto de riscos envolvidos em relação à autodeterminação informativa digital e aos institutos jurídicos que a procuram proteger, essenciais para o desenvolvimento da sociedade do presente e do futuro.

Sem qualquer intenção de esgotar o tema, faremos uma abordagem inicial sobre a autodeterminação digital, o conceito, evolução e abrangência atual, bem como a sua aplicação no âmbito da proteção de dados pessoais de saúde, tendo em consideração a normatização da matéria, especialmente no Direito da União Europeia e português. Em seguida, examinaremos o impacto da pandemia na autodeterminação informativa, nomeadamente quanto às ameaças que surgiram com os diversos instrumentos tecnológicos de monitorização digital.

A partir dessas premissas, procuraremos enfrentar o caso específico dos passaportes vacinais, a sua adoção como forma de viabilizar o retomar das atividades numa sociedade impactada pela pandemia, constituindo alternativa às medidas de *lock down.*

Nesse ponto, é bom registar, o presente trabalho não cuidará das polémicas sociais e éticas geradas pela legislação que favorece, estimula e em alguns casos impõe às pessoas a vacinação contra a COVID-19; limitar-nos-emos ao âmbito do impacto dessas medidas na autodeterminação informativa e aos princípios que a presidem.

2. AUTODETERMINAÇÃO INFORMATIVA EM UM MUNDO DIGITAL – OS DADOS PESSOAIS DE SAÚDE E SUA PROTEÇÃO NO DIREITO DA UNIÃO EUROPEIA E NO DIREITO PORTUGUÊS

Vive-se uma era digital. Os recentes progressos tecnológicos transformam profundamente a sociedade, constituindo o divisor de águas que sinaliza o início de um tempo em que a transmissão de informações se dá em velocidade e quantidade nunca vistas.

A tecnologia desenvolvida renova-se a cada dia, à medida que se populariza e leva toda a sociedade a participar, queira-se ou não, dessa teia de comunicação chamada internet. É a sociedade da comunicação.

As tecnologias digitais de informação e comunicação (chamadas TDICs, ou, em inglês, ICT, acrónimo para *Information Communication Technologies*) amplamente difundidas, não mais exclusivas de alguns e já quase totalmente portáteis, assumem novas dimensões, públicas e privadas, ocupam espaços antes inimagináveis; são o principal meio para realizar a interatividade e a interconectividade, promover a globalização e ampliar a velocidade de acesso aos dados. Por outro lado, as informações são armazenadas numa 'memória coletiva' cujos limites tendem ao infinito. Estabelecem-se novas relações entre as pessoas, absolutamente desvinculadas de tempo e espaço; criam-se inauditas experiências e novas práticas sociais. Enfim, está em curso, e com a perspetiva de cada vez mais se acentuar, a revolução da informação (também conhecida como era tecnológica ou terceira revolução industrial).

Todo este movimento e os seus efeitos na vida da sociedade e do cidadão não são ignorados pelo Direito, que precisa tutelar as relações jurídicas nascidas sob o pálio dessa nova realidade. No campo do Direito Privado, há reflexos notáveis no Direito Laboral, nos Direito dos Contratos, no Direito Bancário e assim por diante.

Ainda no campo do Direito Privado, merecem especial destaque os chamados direitos da personalidade, que são a projeção concreta do princípio constitucional da dignidade da pessoa humana[6] [7].

2.1. DIREITOS DA PERSONALIDADE, DIREITO À PRIVACIDADE E DIREITO DA PROTEÇÃO DE DADOS

M.R. Guimarães e M.R. Redinha[8] salientam que o aumento exponencial do uso da Internet, com o surgimento das redes sociais, criou desafios "*ao arcabouço jurídico em relação à privacidade*". E acrescentam, distinguindo bem o direito de personalidade geral (fundamental) dos demais direitos da personalidade, que sobre aquele se apoiam*: "No âmbito jurídico português, esses instrumentos envolvem direitos fundamentais previstos tanto no direito cons-*

[6] Artigo 1.º da Constituição da República Portuguesa – Disponível em https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx Consultado em 16 de fevereiro de 2022.

[7] Sobre o princípio constitucional da dignidade da pessoa humana, veja-se Jorge Miranda – *A Constituição e a dignidade da pessoa humana*. Lisboa: Didaskalia, 1999. p. 473-485. e Fernando António Rodrigues Da Silva Coutinho Oliveira, **–** *Breves considerações a respeito do princípio da dignidade da pessoa humana* Disponível em https://sigarra.up.pt/fdup/pt/pub_geral.pub_view?pi_pub_base_id=24817**-** Consultado em 10.06. 2022.

[8] Cf. Maria Raquel Guimarães e Maria Regina Redinha – *A Portuguese Approach to Privacy in COVID-19 Times*: *Through the Keyhole*. Coronavirus and the Law in Europe – Intersentia Online, 2021. Disponível em https://www.intersentiaonline.com/permalink/1fac1271118a21090498ddef1399707b Consultado em 15.01. 2022.

titucional quanto no penal. Os direitos de personalidade, destinados a proteger os interesses da personalidade nas relações privadas, pertencem particularmente ao direito civil, mas também protegem os indivíduos nas áreas do trabalho e do direito penal. As diferentes camadas de proteção oferecidas por esses instrumentos legais funcionam de forma complementar, muitas vezes sobrepostas a fim de proteger os diversos níveis de intrusão que afetam os interesses da personalidade. Este intrincado conjunto de ferramentas inclui um "direito de personalidade geral", uma cláusula geral que estabelece o direito ao livre e pleno desenvolvimento da personalidade, um direito fundamental onde todos os interesses conhecidos e desconhecidos, previsíveis e imprevisíveis da personalidade humana podem estar envolvidos, com base no artigo 70 do Código Civil. Esta norma permite uma atualização permanente do direito civil no contexto em evolução e dinâmica dos direitos da personalidade, esticando sua capacidade de enfrentar novos desafios e crises imprevisíveis em um mundo em mudança. Ao mesmo tempo, o Código também introduz um direito especial de personalidade, protegendo expressamente a "intimidade da vida privada", afirmando que a extensão da proteção depende da natureza do caso e da condição da pessoa."

Orlando de Carvalho pondera que o direito geral da personalidade não deve ser confundido com mera ferramenta para superar as possíveis lacunas decorrentes da previsão dos direitos de personalidades especiais; e nem mesmo admite a condensação desses direitos em um só dispositivo. O direito geral da personalidade serve como fundamento axiológico para as demais disposições legais, como referencial interpretativo. [9]

Para Caio Mário da Silva Pereira, a personalidade não constitui propriamente um direito, senão um ponto em que se apoiam os direitos e obrigações[10]. Elimar Szaniawski, por outro lado, aceita o conceito de direitos da personalidade, que qualifica como os "direitos primeiros", que tutelam a pessoa humana, individualmente considerada, representando a defesa dos atributos da personalidade[11].

Sobre os direitos da personalidade, Jorge Miranda[12], sob outra perspetiva, ensina: "*Os direitos da personalidade remontam, em Portugal, aos "direitos originários" do Código de Seabra, uma das expressões da visão antropocêntrica ou "individuocêntrica" que o enformava, e adquirem hoje consagração formal e nominal no Código Civil de 1966. Não traduzem meras conquistas doutrinárias à margem da lei. Eram "direitos originários" o direito de existência, o direito*

---

[9] Cf. Orlando De Carvalho, in *Teoria Geral do Direito Civil.* 3ª ed. Coimbra: Coimbra Editora, 2012, p. 26.

[10] Cf. Caio Mario Da Silva Pereira, – *in Instituições de Direito Civil*. 19ª ed. Rio de Janeiro: Forense, 2002, p. 154.

[11] Cf. Elimar Szaniawski – *in Direitos de personalidade e sua tutela*. São Paulo: Revista dos Tribunais, 1993, p.11

[12] Cf. Jorge Miranda – *in Curso de Direito Constitucional***.** Lisboa: Universidade Católica Editora, 2016, 2, p. 58.

de liberdade, o direito de associação, o direito de apropriação e o direito de defesa (arts. 359.º e segs. do Código de 1867). E atualmente preveem-se, além da tutela geral da personalidade (art. 70.º do Código de 1966), a proteção contra a ofensa a pessoas já falecidas (art. 71.º), o direito ao nome e ao pseudônimo (arts. 72.º e 74.º) a reserva do conteúdo de cartas-missivas e outros escritos confidenciais (arts. 75.º, 76.º e 77.º), o direito à imagem (art. 79.º) e a reserva sobre a intimidade da vida privada (art. 80.º) – a que podem ainda ser aditados outros direitos."

O jurista enuncia, em seguida, os direitos da personalidade: "*II – Para lá do postulado primordial do respeito da dignidade da pessoa humana (art. 1.º da Constituição), com tudo quanto implica, eles dir-se-iam corresponder a direitos como o direito à vida (arts. 24.º e 33.º, n.º 4), o direito à integridade pessoal (art. 25.º), os direitos ao desenvolvimento da personalidade, à capacidade civil, ao bom nome e reputação, à imagem, à palavra e à reserva da intimidade da vida privada (art. 26.º, n.º 1), o direito à liberdade e à segurança (art. 27.º), certas garantias relativas à informática (art. 35.º), o direito de resposta (art. 37.º), a liberdade de consciência, de religião e de culto (art. 41.º), a liberdade de criação cultural (art. 42.º), a liberdade de aprender e ensinar (art.43.º), a liberdade de escolha de profissão (art. 47.º, n.º 1), o direito ao trabalho (art. 58.º), o direito ao ambiente (art. 66.º), o direito à educação e à cultura (art. 73.º) e o direito à cultura física e ao desporto (art. 79.º). Não obstante largas zonas de coincidência, não são, contudo, assimiláveis direitos fundamentais e direitos de personalidade. Basta pensar nos demais direitos inseridos no texto constitucional que extravasam dali: o direito de acesso aos tribunais (art. 20.º, n.º1), o direito à cidadania (art. 26.º, n.º 1), as garantias da liberdade e da segurança (arts. 28.º e segs.), a grande maioria dos direitos, liberdades e garantias e dos direitos econômicos, sociais e culturais (arts. 58.º e segs.) ou os direitos fundamentais dos administrados (art. 268.º). Mas, sobretudo, são distintos o sentido, a projeção, a perspetiva de uns e outros direitos. Os direitos fundamentais pressupõem relações de poder, os direitos de personalidade relações de igualdade. Os direitos fundamentais têm uma incidência publicística imediata, ainda quando ocorram efeitos nas relações entre particulares (como prevê o art. 18.º, n.º 1, a ser estudado a seu tempo); os direitos de personalidade uma incidência privatística, ainda quando sobre ou subposta à dos direitos fundamentais. Os direitos fundamentais pertencem ao domínio do Direito constitucional, os direitos de personalidade aos do Direito civil*."

No direito da personalidade geral, estão abrangidos, assim, os direitos especiais à reserva da intimidade da vida privada[13], ao bom nome, à

[13] O direito à privacidade foi destacado, talvez pela primeira vez, num artigo publicado em 15.12.1890, por Samuel D. Warren e Louis Brandeis. No artigo, os autores destacaram que o direito da *common law*, que antes se preocupava apenas com a proteção física do indivíduo e dos seus bens (terra e rebanho), deveria abranger também o direito de aproveitar a vida (*enjoy life*) e o "direito de ser deixado em paz" (*right to be let alone*), em resposta às

reputação, à imagem, e a um conjunto de "garantias relativas à informática". Esses direitos e garantias, intimamente vinculados ao princípio da Dignidade da Pessoa Humana[14], previstos e protegidos na Declaração Universal dos Direitos do Homem, de 10.12.1948 (art. 12.º) e na Convenção Europeia dos Direitos do Homem, de 04.11.1950 (art. 8.º), assim como na Carta dos Direitos Fundamentais da União Europeia (arts. 7.º e 8.º) e no Tratado sobre o Funcionamento da União Europeia (art. 16.º – ex artigo 286 TCE), dão amplo respaldo, na perspetiva do mundo informático, a um novo ramo do direito, que se passou a denominar Direito da proteção de dados. Essa denominação é sujeita a muitas e pertinentes críticas, uma vez que não se trata apenas de se protegerem os dados, mas também de regular o seu tratamento.[15]

Menezes Cordeiro[16] afirma que "*A expressão Direito da proteção de dados aponta, como acima referido, para uma funcionalização originária deste ramo jurídico dirigida à proteção da posição jurídica dos titulares dos dados e dos seus respetivos direitos. Todavia não é assim: tanto numa perspetiva história, como numa perspetiva dogmática atual, a produção legislativa relativa aos dados pessoais justificou-se não para acautelar os interesses individuais dos titulares dos dados – esses seriam sempre protegidos através da invocação de normas gerais relativas ao direito da personalidade – mas para regular o seu tratamento. Não se nega, naturalmente, que o direito à autodeterminação informacional e a sua proteção desempenham um papel nuclear, somente se contesta: (i) que este se encontre funcionalizado a esse único propósito; e (ii) que foram essas as rationes subjacentes à sua emergência e autonomia, enquanto ramo jurídico próprio*."

Seja qual for a denominação que se queira dar a esse novo ramo do direito, o que releva é a sua proposta de regulamentar o tratamento dos dados das pessoas singulares[17], com a segurança da obediência ao direito

práticas da época, de fotografia e jornalismo. Cf. Samuel D. Warren e Louis Brandeis -*in The Right to Privacy*. Harvard Law Review, Vol. IV, 15.12.1980 Disponível em https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.ht ml – Consultado em 28.02.2022.

[14] Sobre a fundamentação do direito à proteção de dados e sua ligação com a Declaração Universal dos Direitos do Homem, Lurdes Dias Alves, *in Proteção de Dados Pessoais no Contexto Laboral*. Coimbra: Almedina, 2020. Pp. 13-14.

[15] Neste sentido é a lição de A. Barreto Menezes Cordeiro – *in Direito da proteção de dados: à luz do RGPD e da Lei n.º 58/2019*. Coimbra: Almedina, 2020. p. 32, para quem : "Apesar da sua rápida consolidação, a locução *Direito da proteção de dados* foi criticada por parte relevante da primeira doutrina especializada. Smitis e Bull descrevem o termo como sendo enganador, por transmitir uma ideia incorreta do seu objeto de estudo. Steinmüller, igualmente crítico da nomenclatura, sugere uma alternativa: o Direito da proteção da informação (*Informationsshutz*).

[16] Cf. A. Barreto Menezes Cordeiro, *ob. cit*., p. 33.

[17] Segundo o artigo 4.º, inciso 2, do RGPD, a definição jurídica de Tratamento é "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou

à privacidade[18], à imagem e ao livre desenvolvimento da personalidade, entre outros, estimulando o titular dos dados a exercer o controlo, tanto quanto possível, do uso que tais informações possam sofrer, para concretização da autodeterminação informacional a que se refere Menezes Cordeiro. Colima-se, assim, impedir que o acesso indevido aos dados possa ser causa de discriminação,[19] sem opor demasiados obstáculos à circulação desses dados, essencial à fruição dos benefícios decorrentes do avanço da tecnologia.

A questão é relevante pois envolve, não apenas aspetos pessoais, mas uma riqueza em patamares inéditos, que move interesses transnacionais poderosíssimos.

Segundo Jorge M. Carvalho, "os dados pessoais são, atualmente, considerados o novo ouro ou o novo petróleo, sendo um importante bem transacionável" (…).[20] Os dados passaram a ser a nova "*commodity*", fonte de riqueza para a era digital [21]

Diante de interesses financeiros e empresariais poderosos é que se contrapõe o direito do cidadão de exercer o controlo do uso de suas

alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição". Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32021R0953&from=PT

[18] Cf. Paulo Mota Pinto *in – Direitos de Personalidade e Direitos Fundamentais: estudos*. Coimbra: Gestlegal, 2018. p. 508. O autor defende que a privacidade assegura o desenvolvimento da individualidade e das relações humanas de confiança, motivo pelo qual é comumente associada a um aspeto da dignidade humana.

[19] Carlos Nelson Konder – *in O tratamento de dados sensíveis à luz da Lei 13.709/2018. – Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.* São Paulo: Thomson Reuters Brasil, 2019. P. 451 : "Privacidade como autodeterminação informativa/existencial e reconhecimento da construção dinâmica da identidade pessoal conjugam-se, assim, como novas formas de manifestação da proteção jurídica da pessoa humana contra as ameaças e estigmatização e discriminação oriundas do desenvolvimento tecnológico. Com efeito, a principal preocupação com relação ao armazenamento e circulação de informações relativas à pessoa humana diz respeito à sua utilização para submetê-la a estigmas, viabilizando sua discriminação perante as demais. Entre os diversos dados relativos à pessoa, alguns são especialmente idôneos a facilitar processos sociais de exclusão e segregação, razão pela qual seu controle deve ser ainda mais rigoroso. Essa é a chave de leitura adequada para compreender a qualificação de dados pessoais como sensíveis".

[20] Jorge Morais Carvalho – in Manual de Direito do Consumo. 6ª ed. Coimbra: Almedina, 2019. ISBN 978-972-40-7833-5. P.56.

[21] *In* The Economist, 06.05. 2017: *The world most valuable resource is no longer oil but data*: "*A NEW commodity spawns a lucrative, fast-growing industry, prompting antitrust regulators to step in to restrain those who control its flow. A century ago, the resource in question was oil. Now similar concerns are being raised by the giants that deal in data, the oil of the digital era. These titans—Alphabet (Google's parent company), Amazon, Apple, Facebook and Microsoft—look unstoppable. They are the five most valuable listed firms in the world".* Disponível em https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data . Consultado em 28.01. 2022.

informações, a autodeterminação informacional. Em tempos de pandemia, todo esse tema entra em ebulição em vista do tratamento, em larguíssima escala, das informações pessoais relativas à saúde.

Dados muito valiosos e em quantidade incalculável são obtidos diretamente dos seus titulares a todo o momento e sujeitos a tratamento, sob a justificativa de se fazer necessário o combate à disseminação do vírus. É claro o risco para os titulares desses dados e quase inevitável verificar-se o cenário antevisto por Harari, de que tais dados deem ensejo a um monitoramento da população, seja por autoridades ou empresas, ou mesmo por empregadores em relação a seus empregados, avançando sobre conquistas caras da sociedade.

2.2. AUTODETERMINAÇÃO INFORMATIVA DIGITAL – CONCEITO, EVOLUÇÃO E ABRANGÊNCIA

Conforme esclarece Menezes Cordeiro[22], o termo ´autodeterminação informacional` designa, na Alemanha, a subjetivação da posição jurídica do titular de dados pessoais e teria sido cunhado, pela primeira vez, por Steinmüller e lá consagrada pelo Tribunal Constitucional Federal. [23]

Segundo o jurista, a discussão que gerou a definição desse conceito jurídico teria ocorrido em acórdão do *BVerfG* sobre uma lei alemã que tinha por objetivo permitir a coleta de informações pessoais de variadas naturezas – a Lei dos Censos, de 1983 – *Volkszählungsgesestzes*. A Suprema Corte germânica teria examinado a referida lei sob o enfoque da sua constitucionalidade e em especial perante os princípios da dignidade da pessoa humana e o livre desenvolvimento da personalidade, presentes na constituição alemã e concluído que o direito ao livre desenvolvimento da personalidade pressupõe: (i) que o titular dos dados saiba quais informações suas são detidas por terceiros, em que momento e contexto; (ii) liberdade de agir, sem que haja um controlo constante das suas ações e decisões. O direito então reconhecido não seria absoluto, pois não haveria um controlo total sobre os dados[24].

Menezes Cordeiro considera que esse seria um *novo direito* e afirma que o Tribunal assim procedeu à sua concretização: "(i) em princípio, cabe ao próprio titular determinar em que termos os seus dados pessoais podem

---

22 Cf. A. Barreto Menezes Cordeiro, *ob. cit*., p. 257

23 *Bundesverfassungsgericht* ou, simplesmente, *BVerfG*.

24 A respeito deste tema, veja-se a premissa estabelecida pelo TJUE no acórdão proferido no julgamento dos processos apensos C-92/09 e C 93/09 (itens 47 e 48), *verbis*: "A este respeito, sublinhe-se que o artigo 8.°, n.º 1, da Carta estabelece que «[todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito». Este direito fundamental está indissociavelmente relacionado com o direito ao respeito da vida privada consagrado no artigo 7.° desta mesma Carta. Todavia, o direito à protecção dos dados pessoais não é uma prerrogativa absoluta, mas deve ser tomado em consideração relativamente à sua função na sociedade (v., neste sentido, acórdão de 12.06. 2003, Schmidberger, C-112/00, Colect., p. I-5659, n.° 80 e jurisprudência aí referida)."

ser divulgados e tratados; (ii) as restrições ao direito à autodeterminação informacional apenas podem ocorrer quando fundadas no interesse público e encontrarem suporte constitucional bastante – o princípio da proporcionalidade deve a todo tempo ser respeitado; e (iii) a utilização dos dados pessoais deve ser limitada por lei". As dúvidas que teriam seguido à referida decisão eram sobre se esse direito à autodeterminação seria ou não oponível contra todos os terceiros ou somente no âmbito do direito público.

Esclarece-nos, o jurista, ainda, que "os desenvolvimentos viriam a demonstrar a amplitude e transversalidade desse *novo* direito"[25].

Sobre a autodeterminação informativa, merece destaque a posição adotada pelo Supremo Tribunal de Justiça de Portugal no julgamento, pela 5.ª Secção, do recurso no proc. 679/05.7 TAEVR.E2.S1, Relatora Cons. Helena Moniz (16 de outubro de 2014): "o que aqui está em causa, para além da privacidade, é o direito (fundamental) à autodeterminação informativa. Assim sendo, o simples facto de os dados poderem ser públicos não é suficiente para afastar aquela lesão. Neste sentido, constituindo a proteção concedida pelo art. 47.º, da LPDP, uma decorrência do direito à autodeterminação informativa, previsto no art. 35.º, da CRP, este protege uma amplitude de direitos fundamentais para lá do direito à privacidade. O direito à autodeterminação informacional dá "a cada pessoa o direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em «simples objeto de informação»" (Gomes Canotilho e Vital Moreira)".[26]

A autodeterminação informacional "pode impedir que o "eu" seja objeto de apropriação pelos outros, como matéria de comunicação na esfera pública. Nela conjuga –se o direito ao segredo (à intromissão dos outros na esfera privada, com tomada de conhecimento de aspetos a ela referentes) e um direito à reserva (proibição de revelação)".[27]

O Tribunal Constitucional português, no julgamento da constitucionalidade dos artigos 2.º e 3.º Decreto n.º 139/X da Assembleia da República, proferiu o acórdão n.º 442/2007[28] (processo n.º 815/07), sendo Relator o Conselheiro Joaquim de Sousa Ribeiro, em que ficou assente que:

"*Das três manifestações em que se fracciona o conteúdo do direito à reserva da intimidade da vida privada e familiar – direito à solidão, direito ao anonimato, e autodeterminação informativa – é esta última a sua expressão cimeira e mais relevante, e aquela que particularmente nos interessa quando está em causa o estatuto constitucional do sigilo bancário.*

---

[25] Cf. A. Barreto Menezes Cordeiro, *ob. cit.,* p. 259

[26] Cf. Gomes Canotilho e Vital Moreira – *in Constituição da República Portuguesa Anotada*. 4.ª ed. Coimbra: Coimbra Editora, 2007. Vol. 1, p. 551.

[27] Cf. J. Ribeiro Sousa. -*in* A tutela de bens da personalidade na Constituição e na jurisprudência constitucional portuguesas. In *Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho***.** Coimbra: Coimbra Editora. Vol. III, p. 853.

[28] Disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20070442.html 15.03.2022

Por autodeterminação informativa poderá entender-se o direito de subtrair ao conhecimento público factos e comportamentos reveladores do modo de ser do sujeito na condução da sua vida privada. Compete a cada um decidir livremente quando e de que modo pode ser captada e posta a circular informação respeitante à sua vida privada e familiar."

E em recente acórdão daquela mesma Corte Constitucional sobre a polémica questão dos metadados[29], ficou assente o respeito à autodeterminação informativa, decorrente do direito ao sigilo de dados pessoais e inerente ao livre desenvolvimento da personalidade, como se vê do seguinte trecho do voto do Relator: "*Ademais, mesmo fora do domínio das comunicações, o direito ao livre desenvolvimento da personalidade abrange o direito ao sigilo dos dados pessoais — que, como se viu, não compreende somente aqueles que diretamente identificam uma pessoa, mas também aqueles que, sem esforço excessivo, permitam chegar a essa identificação — como se concluiu no Acórdão n.º 464/2019: «Pode, na verdade, afirmar-se que o segredo dos dados pessoais e o poder de controlo do sujeito sobre os mesmos constituem uma garantia do direito ao livre desenvolvimento da personalidade enquanto possibilidade de «interiorização autónoma» da pessoa ou o direito a «autoafirmação» em relação a si mesmo, contra quaisquer imposições heterónomas (de terceiros ou dos poderes públicos). Este direito à "autoafirmação" dá guarida a vários «direitos de personalidade inominados mesmo que não especificamente positivados na Constituição, como por exemplo, o direito aos documentos pessoais e o direito à autodeterminação informativa quanto a dados pessoais constantes de ficheiros manuais ou informáticos, o direito à confidencialidade de dados pessoais constantes de atos ou decisões públicas respeitantes ao estado civil, o direito de não ser espiado no desenvolvimento de atividades lícitas (cf. Gomes Canotilho/Vital Moreira, Vol. I, ob. cit., pp. 464-465».*

Interessa-nos especificamente a autodeterminação informativa (ou informacional) que se realiza no mundo digital onde atualmente estão, como já visto, os maiores riscos para a privacidade e o desenvolvimento da personalidade dos cidadãos, até por estar aí armazenada eletronicamente uma quantidade de informações pessoais que nem mesmo os próprios cidadãos supõem e que, muitas vezes, lhes são completamente desconhecidas. É a autodeterminação digital, da qual cuida o presente estudo.

---

[29] Tribunal Constitucional, Processo n.º 828/2019, acórdão n.º 268/2022, Plenário, Relator Conselheiro Afonso Patrão, julgado em 04.2022. O Tribunal declarou a inconstitucionalidade das normas dos artigos 4.º e 6.º da Lei n.º 32/2008, de 17 de julho, que determinam a conservação, pelos fornecedores de serviços de telecomunicações e comunicações eletrónicas, de todos os dados de tráfego e de localização relativos a todas as comunicações ou sua tentativa, pelo período de um ano, com vista à sua eventual futura utilização para prevenção, investigação e repressão de crimes graves.

2.3. UNIÃO EUROPEIA E PORTUGAL – O RGPD E A LEGISLAÇÃO PORTUGUESA

O direito à proteção dos dados pessoais, como se viu em cima, é considerado um direito fundamental na União Europeia e está previsto na Carta dos Direitos Fundamentais da União Europeia (CDFUE), especificamente no seu artigo 8.°, assim como no artigo 16.°, n.° 1, do Tratado sobre o Funcionamento da União Europeia (TFUE). Vincula-se intimamente ao próprio direito à privacidade, previsto no artigo 7.º da CDFUE.

Merece ainda ser mencionada a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, que foi o primeiro instrumento internacional no domínio da proteção de dados[30] e tinha por objetivo "garantir [...] a todas as pessoas singulares [...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal".[31]

No campo do direito derivado[32], a partir da década 90, a Comunidade Europeia passou a adotar novos mecanismos legais para a proteção dos dados pessoais; destaca-se a Diretiva 95/46/CE (Diretiva do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados), que estabeleceu as condições para o tratamento dos dados pessoais e os direitos dos titulares e previu a criação de órgãos independentes para o controlo nos Estados-Membros[33].

Já no século XXI, adotou-se a Diretiva 2002/58/CE de 12 de julho de 2002[34], relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, a complementar as regras da Diretiva 95/46. Em 2008, veio a Decisão-Quadro 2008/977/JAI que regulamentou a proteção dos dados pessoais no domínio da cooperação judiciária em matéria penal e policial.

---

30 Informação constante em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf (acedido em 10.01.2022)

31 A Convenção foi recentemente modernizada com a adoção do Protocolo de Modificação CETS n.º 223 a 18 de abril de 2018. Disponível em https://rm.coe.int/16808ade9d. 15.03.2022

32 – O Direito derivado ou secundário é "o corpo legislativo que decorre dos princípios e objetivos consagrados nos Tratados" e "inclui regulamentos, diretivas, decisões, recomendações e pareceres". Definição encontrada no site institucional da Comissão Europeia – https://ec.europa.eu/info/law/law-making-process/types-eu-law_pt 15.03.2022

33 A Diretiva95/46/CE foi revogada a partir de 25 de maio de 2018, pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

34 Esta Diretiva foi alterada pela Diretiva2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006. Porém, esta última Diretiva veio a ser considerada inválida pelo Tribunal de Justiça, por violação grave do princípio da proporcionalidade, à luz dos artigos 7.º, 8.º e 52.º n.º1 da Carta (Tribunal de Justiça da UE, Grande Secção, acórdão de 8 de abril de 2014, – processos apensos C-293/12 e C-594/12. Disponível em https://curia.europa.eu/juris/liste.jsf?language=pt&num=C-293/12. 15.03.2022

Em 2016, toda a regulamentação jurídica relativa à proteção de dados na União Europeia foi revista e os conceitos consolidados em Regulamento (Regulamento UE 2016/679, conhecido como Regulamento Geral sobre Proteção de Dados – RGPC)[35] [36]. O RGPD entrou em vigor no dia 25 de maio de 2016 simultaneamente, em todos os Estados Membros da União Europeia. Como se trata de um Regulamento, não houve necessidade de transposição para o direito interno, impondo-se a disciplina uniformizada para os Estados Membros em maio de 2018, data em que terminou o período transitório de dois anos para que se desse a necessária conformação com as obrigações ali previstas (muitas das quais, é bom que se diga, já existiam sob a égide da Diretiva 95/46/CE).

O RGPD é um instrumento para a unificação do direito da proteção de dados nos Estados-Membros, com o objetivo de possibilitar uma aplicação homogénea do direito no limite territorial da União, para assim consolidar o Mercado Único. De lembrar que, de acordo com o artigo 288.ª do TFUE, "(...) O regulamento tem caráter geral. É obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.", o que lhe permite unificar o direito regulado de uma só vez em todos os Estados-Membros, independentemente de se abrir espaço, no próprio RGPD, para que o legislador de cada Estado-Membro possa atuar nas chamadas cláusulas de abertura que vão concretizar o Regulamento e permitir a sua adaptação às características e necessidades locais.

Também merece ser destacado o Regulamento UE 2018/1725, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados. O RGPD previa a adaptação do Regulamento (CE) n.º 45/2001 a fim de garantir um regime de proteção de dados sólido e coerente na União e de permitir a sua aplicação em paralelo com o RGPD. Foi esse o objetivo concretizado pelo Regulamento 2018/1725.

E é nessa perspetiva que atua o legislador português, editando regras de execução do RGPD no âmbito nacional, sempre nos limites das cláusulas de

[35] – Revogou a Diretiva95/46, a Diretiva (UE) 2016/680 e a Decisão-Quadro 2008/977/JAI, sendo aplicável a partir de 25 de maio de 2018.

[36] Quanto às instituições e órgãos da União vinculados especificamente à proteção de dados, situação que era regida pelo Regulamento (CE) n.° 45/2001, foi criado novo cenário, com a edição do Regulamento (UE) 2018/1725, que revogou o anterior desde 11 de dezembro de 2018 e procurou harmonizar a matéria com o RGPD.

abertura estabelecidas pelo Regulamento e com respeito aos princípios ali estabelecidos[37] [38].

No âmbito do direito interno, é bom destacar que o tema da proteção de dados, como já visto, tem fundamento constitucional. Segundo Menezes Cordeiro[39], "o Direito constitucional português tem uma longa tradição na regulamentação dos dados pessoais e do seu tratamento. A Constituição da República Portuguesa terá sido, à luz dos elementos recolhido, a primeira Lei Fundamental a reconhecer, diretamente, alguma proteção constitucional aos titulares de dados pessoais. O núcleo embrionário do Direito da proteção de dados contemporâneos surgia já na versão original do artigo 35.º da CRP".

Segundo o jurista, a atual redação do artigo 35.º, a partir da Revisão Constitucional de 1997, teria sido motivada pelo conteúdo da Diretiva n.º 95/46[40]. Seja como for, a norma constitucional é bastante clara ao assegurar o direito ao conhecimento das informações pessoais pelo seu titular, à sua retificação e atualização, ao remeter à lei o estabelecimento das condições para o tratamento automatizado, conexão, transmissão e utilização desses dados, garantindo a sua proteção.

No plano da legislação ordinária portuguesa, a primeira menção se faz ao artigo 70.º, n. 1.º, do Código Civil de 1966, que institui uma cláusula geral para assegurar os direitos da personalidade e proteger seu titular contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral. Segundo Paulo Mota Pinto[41], este direito confere uma tutela geral que, além e se ajustar melhor à complexidade da personalidade humana, pode abranger bens da personalidade não tipificados em lei. Por isso mesmo, o direito da personalidade seria "aberto, sincrônica e diacronicamente, permitindo a tutela de novos bens, e face a renovadas ameaças à pessoa humana".

Para além do Código Civil, pode-se destacar a Lei n.º 2/73, de 10 de fevereiro, e o Decreto-Lei n.º 555 /73, de 26 de outubro[42]. No início da década de 90, foi publicada a Lei 10/91, de 29 de abril, voltada especificamente para a "proteção de dados pessoais face à informática". Essa lei foi revogada pela Lei n.º 67/98

---

37 Em caso de contradição entre o Regulamento e a lei interna dos Estados-Membros, deve prevalecer o direito europeu, como ficou assente no julgamento pelo TJUE do processo C-106/77 (acórdão de 09.03.1978 – Simmenthal), *verbis*, "O juiz nacional responsável, no âmbito das suas competências, por aplicar disposições de direito comunitário tem obrigação de assegurar o pleno efeito de tais normas, decidindo, por autoridade própria, se necessário for, da não aplicação de qualquer norma de direito interno que as contrarie, ainda que tal norma seja posterior, sem que tenha de solicitar ou esperar a prévia eliminação da referida norma por via legislativa ou por qualquer outro processo constitucional".

38 Disso decorre a especial relevância aos 173 considerandos (*consideranda*), que ajudam a interpretar os artigos do Regulamento, expressando-se em todas as suas 24 versões.

39 Cf. A. Barreto Menezes Cordeiro, *ob. cit*., p.73

40 Cf. A. Barreto Menezes Cordeiro, *ob. cit*., p. 75

41 Cf. Paulo Mota Pinto, *ob. cit.* p. 493/494.

42 Ambos os diplomas tratavam do Registo Nacional de Identificação e já cuidavam da proteção de dados pessoais.

(Lei de Proteção de Dados Pessoais) que, por sua vez, veio a ser substituída pela lei que hoje disciplina a matéria no âmbito do direito interno – a Lei n.º 58/2019, de 08 de agosto, também conhecida como a Lei de Execução do RGPD[43].

Por fim, também merece referência a Lei n.º 27/2021 de 17 de maio, que institui a Carta Portuguesa de Direitos Humanos na Era Digital e que contém regras aplicáveis ao direito da proteção de dados digitais. Essa Lei contém muitas regras programáticas, repete princípios e direitos fundamentais já consagrados (liberdade de expressão, sigilo das telecomunicações, proteção de dados, identidade e bom nome, ciber segurança, entre outros); trazendo parca inovação ao ordenamento jurídico português. Os temas ali tratados já o haviam sido e de forma exaustiva pela Constituição da República, pelos Regulamentos e Diretivas da União e pela própria legislação nacional.[44]

Todos esses diplomas tiveram como uma das suas principais finalidades dar efetividade ao direito fundamental à proteção de dados pessoais, incorporando ao ordenamento jurídico os meios e instrumentos jurídicos próprios para garantir que fosse alcançado tal objetivo.

A proclamação de princípios jurídicos, como se fez no artigo 5.º do RGPD, o estabelecimento de regras específicas para autorizar o tratamento lícito de dados, inclusive no que respeita ao consentimento para esse tratamento, quando exigível, como está bem disciplinado nos artigos 6.º a 11.º do RGPD, a enunciação de direitos do titular dos dados nos artigo 12.º a 23.º do RGPD, bem como de obrigações para aquele responsável pelo tratamento dos dados pessoais previstas nos artigos 24.º a 31.º, tudo isto gera concretude e municia o titular de dados pessoais de instrumentos para que seus direitos sejam respeitados e, tanto quanto possível, possa exercer, na forma prevista na lei, a autodeterminação informativa digital.

Parece importante relevar o direito de informação e de acesso (arts. 13.º, 14.º e 15.º do RGPD), assim como o direito de retificação, de apagamento e de oposição (arts. 16.º, 17.º e 21.º do RGPD). São direitos subjetivos fundamentais para o exercício da autodeterminação informativa, em conformi-

---

43 – Há outros diplomas mais específicos, mas que também cuidam da proteção de dados pessoais, como a Lei n.º 41/2004 (dados pessoais e privacidade nas telecomunicações), Lei n.º 1/2005, de 10 de janeiro e diplomas subsequentes (videovigilância), Lei n.º 12/2005 (informação genética pessoal e dados de saúde), Lei n.º 59/2019, de 08 de Agosto (prevenção, deteção, investigação ou repressão a infração penal).

44 A Comissão Nacional de Proteção de Dados – CNPD, em parecer produzido a respeito do Projeto de Lei n.º 473/XIV/1.ª da AR (parecer 2020/116 de 28 de setembro de 2020), que veio dar origem à Lei n.º 27/2021, apresentou severas críticas ao projeto e destacou que "não obstante a invocação de um extenso conjunto de instrumento jurídicos, a maior parte deles de cariz internacional ou europeu, e de outras iniciativas de debates sobre a matéria, no articulado do Projeto parece esquecer-se que muitos dos direitos, aqui consagrados como digitais, já estão reconhecidos, e com um âmbito bem delimitado, em instrumentos jurídicos vinculativos para o Estado português. E, portanto, consagrados e delimitados em termos tais que não podem agora, no plano legislativo nacional, ser alterados, mesmo que num sentido expansivo das posições subjetivas dos titulares dos dados."

dade com o conceito empregado pelo Tribunal Constitucional Português no acórdão acima citado, que envolveria o "direito de subtrair ao conhecimento público factos e comportamentos reveladores do modo de ser do sujeito na condução da sua vida privada".

2.4. CONCEITO JURÍDICO DE DADOS PESSOAIS DE SAÚDE NO RGPD E NA LEGISLAÇÃO PORTUGUESA

O conceito de dados pessoais está claro no artigo 4.º, 1) do RGPD: "«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

A definição é bastante clara, não obstante possa suscitar, concretamente, diversas questões sobre a extensão dos seus elementos conceituais.

O primeiro elemento adotado pelo RGPD merece especial reflexão: que tipo de informação seria abrangida pelo instituto jurídico? Menezes Cordeiro[45] defende que a aceção a ser atribuída à expressão seja a mais ampla, ultrapassando os limites adotados pelo direito de personalidade, de tal forma que abranja todas as informações relativas à pessoa singular. O jurista se apoia em decisão do Tribunal Constitucional alemão, de que não haverá informação pessoal, "por muito insignificante ou fútil que possa parecer" que não mereça a proteção jurídica. E conclui o argumento ao referir-se a várias decisões do Tribunal Europeu dos Direitos Humanos, em que se consideram abrangidas no conceito de dados pessoais as informações relativas à vida privada bem como as que concernem à vida profissional e social.

De entre todas essas decisões do TEDH acima referidas, merece especial destaque a proferida no julgamento do caso AMANN v. SWITZERLAND (Application n.º 27798/95), de 16 de fevereiro de 2000, em que o Tribunal definiu a extensão a ser dada ao conceito de "vida privada", conforme expresso no artigo 8.º, 1, da Convenção Europeia dos Direitos do Homem, e apontou que esse instituto abrange o direito de estabelecer e desenvolver relações com outras pessoas e que não haveria razões que justificassem a exclusão de atividades de índole profissional ou de negócios daquele conceito, com apoio em precedente daquela mesma corte de justiça. Essa interpretação é correspondente à que se atribui ao artigo 1.º da Convenção n.º 108, de 28 de janeiro de 1981, do Conselho da Europa (Convenção para a Proteção de Indivíduos Relativamente ao Tratamento Automático de Dados Pessoais) e que, já então, definia informação pessoal como "qualquer informação relativa a uma pessoa

[45] Cf. A. Barreto Menezes Cordeiro, *ob. cit*., pp. 107 e 108.

identificada ou identificável" (artigos 1.º e 2.º). [46] Essa posição ajuda a definir a extensão de dados pessoais, para abranger todos os dados pertinentes a uma pessoa, não importa qual seja a relevância de tais dados.

Também outro aspeto deve ser destacado. Os dados pessoais compreendidos na proteção do RGPD são os relativos às pessoas singulares, independentemente da sua nacionalidade ou residência. Não abrangem os dados de pessoas coletivas[47]. Igualmente não envolvem aqueles relativos a pessoas falecidas[48], os quais, entretanto, no âmbito de Portugal, são dotados de mecanismos de proteção previstos na lei portuguesa de execução do RGPD[49].

Porém ao presente estudo não interessam todos os dados pessoais, senão uma categoria, que merece mais elevada proteção; os chamados dados especiais ou sensíveis, que, "pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais".[50] São, conforme definição objetiva

---

[46] "The Court reiterates that the storing of data relating to the "private life" of an individual falls within the application of Article 8 § 1 (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48). It points out in this connection that the term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life" (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and the Halford judgment cited above, pp. 1015-16, § 42)."

[47] Não assim as pessoas coletivas, conforme Considerando n.º 14 do RGPD "(14) A proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais. O presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva."

[48] Considerando n.º 27 – "O presente regulamento não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas".

[49] A Lei n.º 58/2019, de 08 de agosto, cuida do tema no seu artigo 17.º, *in verbis*: 1 – Os dados pessoais de pessoas falecidas são protegidos nos termos do RGPD e da presente lei quando se integrem nas categorias especiais de dados pessoais a que se refere o n.º 1 do artigo 9.º do RGPD ou quando se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações, ressalvados os casos previstos no n.º 2 do mesmo artigo. 2 – Os direitos previstos no RGPD relativos a dados pessoais de pessoas falecidas, abrangidos pelo número anterior, nomeadamente os direitos de acesso, retificação e apagamento, são exercidos por quem a pessoa falecida haja designado para o efeito ou, na sua falta, pelos respetivos herdeiros. 3 – Os titulares dos dados podem igualmente, nos termos legais aplicáveis, deixar determinada a impossibilidade de exercício dos direitos referidos no número anterior após a sua morte."

[50] Transcrição de parte do Considerando 51 do RGPD – "Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-

do artigo 9.º, os dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, os dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

É clara a posição de maior fragilidade, pela possível exposição a situações de discriminação ou preconceito (princípio da não discriminação – artigo 21.º da Carta dos Direitos Fundamentais da União Europeia – CDFUE), com possível perturbação dos direitos fundamentais da personalidade, que os titulares de tais dados ostentam, o que justifica plenamente a preocupação do legislador europeu.

Para Canotilho e Moreira, quanto mais os dados refiram-se à personalidade, à dignidade, e à autodeterminação, maior a necessidade de se restringir a recolha e utilização[51].

Os dados pessoais especiais de saúde encaixam-se nesse perfil e, assim, são tratados pelo artigo 4.º, 15, do RGPD que os conceitua como aqueles "relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde".[52] Para Sérgio Deodato, "os dados pessoais de saúde incluem toda a informação relativa à saúde de uma pessoa que é usada pelos profissionais de saúde na sua relação assistencial e que geralmente é registada nos denominados processos clínicos".[53]

Patrícia Cardoso Dias[54], ao tratar dos dados especiais de saúde, leciona que "a especial sensibilidade desta categoria de dados pessoais convoca uma

---

Membros pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais."

51 Cf. Gomes Canotilho e Vital Moreira *Ob. cit.*. p. 557.

52 A Lei n.º 12/2005 de 26 de janeiro no artigo 2.º conceitua do seguinte modo dados de saúde: "todo o tipo de informação direta ou indiretamente ligada à saúde, presente ou futura, de uma pessoa, quer se encontre com vida ou tenha falecido, e a sua história clínica e familiar". A Lei 58/2019 de 8 de agosto, até pela sua própria natureza (de execução de um Regulamento), não contém uma definição de dados especiais de saúde. Porém trata desses dados especificamente nos seus artigos 29.º e 30.º.

53 – Cf. Sérgio Deodato – *in A proteção dos dados pessoais de Saúde*. Lisboa: Universidade Católica Editora. 2017. p. 13.

54 Cf. Patrícia Cardoso Dias – *Proteção* de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da

tutela qualificada atendendo aos impactos negativos que se podem produzir na esfera jurídica pessoal do titular" e que a informação de saúde está "sujeita a um regime de proteção reforçado por corresponder a uma categoria de dados pessoais que é suscetível de gerar ou promover a estigmatização e a discriminação dos respetivos titulares por via da revelação de aspetos da sua fisiologia orgânica que enformam o reduto máximo da privacidade".

São dados sensíveis e por isso mesmo os que sujeitam o seu titular aos maiores riscos de discriminação ou estigmatização, especialmente no ambiente de crise da pandemia.

3. A COVID-19 E A PROTEÇÃO DOS DADOS PESSOAIS DE SAÚDE

3.1. A PANDEMIA DA COVID-19 E SEU IMPACTO NO DIREITO À PROTEÇÃO DE DADOS

Como foi mencionado previamente, um dos impactos relevantes da COVID-19 no sistema jurídico do mundo ocidental deu-se no campo do direito da proteção de dados. A pandemia mostrou-se desafiadora neste ponto, uma vez que, para contenção da doença, os governos deram ênfase à digitalização dos serviços públicos e lançaram mão dos dados de saúde dos cidadãos, necessários para pôr em prática as medidas sanitárias, em quantidade impressionante. Também as empresas privadas desenvolveram novas tecnologias, inclusive de rastreamento de contatos, que proporcionaram a captação cada vez maior de informações (sensíveis) de saúde e, assim, colocaram-se como forças auxiliares dos órgãos públicos, no combate à pandemia.

Com a justificativa, por vezes aceitável e até adequada, de que atuavam com esse objetivo de cooperação, promoveram a captação de dados de saúde e o seu tratamento em níveis que ainda não tinham sido vistos.

Vejam-se os seguintes exemplos.

Em abril de 2020, foi anunciada uma parceria entre a Google e a Apple com o objetivo de disponibilizar uma plataforma, operável tanto no ambiente Android como IOS, que deveria viabilizar o conhecimento dos contatos do usuário (*contact tracing platform*), com a utilização da tecnologia Bluetooth.[55]

proteção de dados de saúde no âmbito da emergência de saúde pública – *in Revista Julgar Online* Janeiro de 2021-1. Disponível em http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/ 28.04.2022.

[55] No anúncio da parceria, foi esclarecido o seguinte: "*Across the world, governments and health authorities are working together to find solutions to the COVID-19 pandemic, to protect people and get society back up and running. Software developers are contributing by crafting technical tools to help combat the virus and save lives. In this spirit of collaboration,*

No comunicado, as empresas destacaram a necessidade de observarem a privacidade e a segurança dos titulares dos dados, assim como respeitar o seu consentimento; anunciaram, também, que as informações do projeto seriam públicas, a viabilizar o controlo por terceiros.

A despeito dessas premissas e compromissos, é inegável que a quantidade de dados de saúde que uma solução tecnológica dessas, desenvolvida com o propósito de combater a pandemia, acaba por absorver é enorme, proporcional ao risco que decorre para a privacidade das pessoas, especialmente no ambiente pandémico. A conjugação de dados de geolocalização com dados sensíveis de saúde em tal magnitude representa um enorme risco para a privacidade.

A Organização Mundial de Saúde (OMS), em manifestação sobre a utilização desse tipo de tecnologia para o combate à pandemia, já ponderava, em 28 de maio de 2020, que: "*Through their products, services or platforms, some private companies capture as much data as governments gather. Such companies may develop or are even sharing their own digital proximity tracking applications with governments and, in some cases, are given the responsibility for collecting and analysing the data thus harvested. Moreover, there is a broader concern that private companies may permanently integrate their commercial products, services and architecture within public health infrastructures.*"[56]

O *The Washington Post*, em 20 de abril de 2020, publicou uma carta aberta do CEO do *Facebook*, Mark Zuckerberg, em que este reconheceu que, com bilhões de usuários, a plataforma reunia as condições para obtenção de dados pessoais em escala mundial, dispondo-se, assim, a utilizar essa situação para captar as informações e fornecê-las aos governos, com o objetivo de ajudar a estruturar estratégias de combate à pandemia. A propósito, veja-se o trecho seguinte da referida carta aberta: *Getting accurate county-by-county data from across the United States is challenging, and obtaining such focused data from across the whole world is even harder. But with a community of billions of people globally, Facebook can uniquely help researchers and health authorities get the information they need to respond to the outbreak and start planning for the recovery*.[57]

Google and Apple are announcing a joint effort to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the virus, with user privacy and security central to the design. Since COVID-19 can be transmitted through close proximity to affected individuals, public health officials have identified contact tracing as a valuable tool to help contain its spread"**.** Disponível em https://www.apple.com/ br/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracingtechnology/ 10.01.2022.

[56] Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing, Interim guidance. Disponível em https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1 06.06.2022.

[57] Disponível em: (https://www.washingtonpost.com/opinions/2020/04/20/how-datacan-aid-fight-against-covid-19/) 15.05.2022

Em reforço dos seus argumentos, Zuckerberg acrescentava "*Data like this can unlock a lot of good. Since we're all generating data from apps and devices every day, there will likely be many more opportunities to use the aggregate data to benefit public health. But it's essential that this is done in a way that protects people's privacy and respects human rights. It's important that organizations involved in this work commit to doing it in a way that protects people's information and that any data collected is used solely for responding to public health emergencies and for other crisis response efforts. Fighting the pandemic has required taking unprecedented measures across society, but it shouldn't mean sacrificing our privacy".*

Estes são, pois, bons e claros exemplos, como nunca, de como as informações pessoais de saúde foram e continuam a ser usadas por empresas e pelos agentes governamentais, por vezes em interação, em quantidade massiva nos momentos de ameaça.

A afirmação de valores e boas intenções, como aquela do FB, de que "*data like this can unlock a lot of good*" ou de que a utilização das informações se deve dar com respeito à privacidade do cidadão, por si só, não são bastantes para afastar os gravíssimos riscos inerentes à opção político-jurídica de se abrirem as portas que protegem os dados pessoais de saúde. Não se pode ser ingénuo a ponto de considerar que tais dados pessoais não possam ser desviados para outras finalidades ou mesmo que sejam objeto de tratamento sem os cuidados que as normas exigem.

Dúvidas existirão sempre sobre os destinos da enorme quantidade de dados coletados, a finalidade da sua utilização (que deve ser exclusivamente o atendimento às medidas de saúde pública emergentes da pandemia) assim como a observância ao princípio da proporcionalidade, que procura afastar os abusos. Assim, também haverá incertezas quanto ao controlo a ser exercido sobre tais condutas e projetos, às medidas para eventual reajuste e ao tratamento dos dados no período pós-pandemia.

Algumas medidas, como a anonimização de dados, sabe-se bem, não são sempre efetivas. Dados anonimizados muitas vezes podem ser "desanonimizados" [58] e até com certa facilidade, com ocorreu em 2006 em relação a dados anónimos fornecidos à NETFLIX[59]. As novas tecnologias e o desenvolvimento assombroso das capacidades informáticas e da inteligência

---

[58] Carissa Vélis – *in Privacidade é Poder, por que razão e como devemos recuperar o controle dos nossos dados, Temas e Debates*. Lisboa: Bertrand Editora Ltda., 2022.

[59] Cf. Carissa Vélis, *ob. cit*. p. 32: "em 2006, a Netflix publicou 10 milhões de classificações de filmes de meio milhão de clientes como parte de um desafio às pessoas para conceberem um melhor algoritmo de recomendações. Os dados eram supostamente anónimos, mas os investigadores da Universidade do Texas, em Autin, provaram que conseguiram reidentificar as pessoas comparando classificações e registos data/hora com a informação na Internet Movie Database (IMBb). Por outras palavras, se vir um filme numa detemrinada noite na Netflix que gostou dele e depois também o classificar na IMDb, os investigadores poderão inferir que foi o leitor o autor das duas classificações."

artificial (IA) reduzem a eficácia das medidas de proteção da privacidade, uma vez que os dados pessoais sejam inseridos na *internet*. Por isso o risco enorme que corremos quando os dados disponibilizados dizem respeito à saúde, por mais justificáveis que sejam os propósitos. E tudo se amplia quando os dados são utilizados pelos governos e por grandes plataformas da *internet*.

Numa situação como a anteriormente descrita, é claro o risco de as informações chegarem às pessoas (singulares ou coletivas) interessadas em fazer delas o comércio de dados que tanto assusta, pela invasão da privacidade e capacidade para gerar discriminações, fraudes, extorsões, além de outras consequências conhecidas. Além disso, há sempre o risco de as próprias autoridades utilizarem esses dados, durante ou depois da pandemia, para fins não estritamente ligados às atividades de saúde pública.

A armazenagem de informações pelas autoridades estatais pode, pois, fazer-se de tal forma que permita o seu uso para outros fins, como se verá mais adiante neste estudo.

Harari, no seu texto já referido, descreveu as medidas drásticas adotadas pela China nos primeiros dias da pandemia com o objetivo de controlar a propagação do vírus. Destacou que, pela monitorização dos *smatphones*, juntamente com centenas de milhões de câmaras de reconhecimento facial e a partir de informações obtidas dos próprios cidadãos sobre a sua temperatura corporal e as condições médicas, as autoridades chinesas puderam, não apenas identificar suspeitos de serem portadores do vírus, como rastrear os seus movimentos e até os seus contatos, enquanto aplicativos alertavam a população contra a proximidade de infetados.

Harari esclarece que esse tipo de tecnologia não estava limitado à Ásia Oriental. Em Israel, o então primeiro-ministro Benjamin Netanyahu autorizou a Agência de Segurança a empregar tecnologia de rastreamento, normalmente dedicada ao combate de terroristas, para vigiar pessoas infetadas por coronavírus, medida que se adotou sob os efeitos de um decreto de emergência[60].

---

[60] Para compreensão da extensão das restrições impostas em Israel, veja-se o artigo da professora Tamar Hostovsky Brandes, "Israel's Perfect Storm: Fighting Coronavirus in the Midst of a Constitutional Crisis – *in* Verfassungsblog on mattrers constitucional. Ressalta-se o seguinte trecho: *The Knesset Service Affairs Committee approved the employment of military cellular tracking technology pursuant to article 7(B)(6), of the General Security Service Law, 5762-2002, which allows the service to perform "activities in any other area determined by the Government, with the approval of the Knesset Service Affairs Committee, which is designed to safeguard and promote State interests vital to the national security of the State". The authorization includes a sunset clause which determines that it will end on April 30th, 2020.The committee required the state to examine less invasive alternatives during this period, and to present them to the committee. The information the Service is allowed to share with the Ministry of Health includes real-time locations of confirmed Covid-19 patients in the 14 days that preceded diagnosis and the personal details of individuals who came into "close contact" with such patients. The Ministry of Health will*

Como se constata, as medidas para enfrentar a pandemia podem, facilmente, prestar-se a desviar os dados de saúde para outros fins perseguidos pelas autoridades estatais ou pelas empresas privadas. O risco é enorme, ainda mais sob a perspetiva proposta por Harari, relativa à realização de monitoramento "*under the skin*".[61]

3.2. FUNDAMENTOS JURÍDICOS PARA A PROTEÇÃO DE DADOS PESSOAIS – APLICAÇÃO, NO AMBIENTE DA COVID-19, DAS REGRAS QUE ESTABELECEM DIREITOS E GARANTIAS DOS TITULARES DE DADOS

Para se antecipar a situações que suscitavam dúvidas sobre a proteção da privacidade, no âmbito das medidas de combate à pandemia, e diante do que dispunha o RGPD em matéria de tratamento de dados pessoais e utilização de dados de localização, assim como relativamente a aspetos inerentes ao ambiente de trabalho, em 19 de março de 2020, o Comité Europeu para a Proteção de Dados expediu uma Declaração sobre o tratamento de dados pessoais no contexto do surto de COVID-19.[62]

A Declaração pretendeu destacar como os dados pessoais estariam protegidos pelas normas vigentes, em especial o RGPD, ante as medidas que se tomavam para evitar a propagação do vírus.

No introito, já se dizia que "*Os governos, assim como as organizações públicas e privadas de toda a Europa, têm estado a tomar medidas para conter e atenuar o surto de COVID-19, que podem implicar o tratamento de vários tipos de dados pessoais. As normas em matéria de proteção de dados (como o Regulamento Geral sobre a Proteção de Dados) não obstam a que sejam adotadas medidas para combater a pandemia de coronavírus. A luta contra as doenças transmissíveis é um objetivo primordial partilhado por todas as nações, devendo ser apoiada da melhor forma possível. A humanidade tem interesse em travar a propagação de doenças e em utilizar técnicas modernas na luta contra os flagelos que afetam grande parte do mundo. Ainda assim, o Comité Europeu para a Proteção de Dados gostaria de sublinhar que, mesmo*

use this information to inform those who came in contact with a Covid -19 patient that they are required to enter isolation.

[61] Yuval Noah Harari, no texto citado, pondera que, no momento em que os estados estão a combater o coronavírus, pode ocorrer a normalização da utilização de instrumentos de vigilância em massa como representar uma transição da vigilância "*over the skin*" (incidente sobre o comportamento exterior, como localização, hábitos, compras, etc) para a "*under the skin*" (capaz de monitorar dados biológicos, como temperatura corporal, pressão arterial, batimentos cardíacos, respiração, etc). A segunda permitiria aos algoritmos saber a condição de saúde antes dos sintomas, antes do próprio cidadão. E, mais ainda, os dados poderiam ser utilizados para avaliação do estado emocional do ser humano, e até, quiçá, dos seus sentimentos, o que representaria uma invasão à privacidade inaudita, podendo gerar discriminações, influências ou manipulações.

[62] Disponível em https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-processing-personal-data-context-covid-19_pt. Consultado em 06.06.2022

nestes tempos de exceção, os responsáveis pelo tratamento dos dados e os subcontratantes devem assegurar a proteção dos dados pessoais dos respetivos titulares."

Destacou igualmente que "*há que ter em conta uma série de considerações para garantir o tratamento lícito dos dados pessoais e ter sempre presente que qualquer medida tomada neste contexto deve respeitar os princípios gerais de direito, não podendo ser irreversível*."

O Comité assinalou, também, que a emergência legitimava a imposição de restrições às liberdades, "desde que sejam proporcionadas e limitadas ao período de emergência." E defendeu, ainda, a aplicação do RGPD, "um diploma legislativo genérico que prevê regras aplicáveis igualmente ao tratamento de dados pessoais num contexto como o do surto de COVID-19", e que "permite que as autoridades competentes em matéria de saúde pública e os empregadores procedam ao tratamento de dados pessoais no contexto de uma epidemia, em conformidade com o direito nacional e nas condições nele estabelecidas". A título de exemplo desse tratamento de dados permitido pelo RGPD, apontou a necessidade "por motivos de interesse público importante no domínio da saúde pública", situação que torna desnecessário obter o consentimento dos particulares.

O entendimento do Comité, ali manifestado, é de que as previsões dos artigos 6.º e 9.º do RGPD são bastantes para autorizar as autoridades públicas competentes, mesmo diante de dados especiais (como os de saúde) a promoverem o respetivo tratamento, para desempenho do mandato legal. Além disso, esclareceu que nas relações laborais o empregador pode, se necessário para cumprir obrigação legal, nomeadamente em matéria de saúde e segurança no local de trabalho, ou por razões de interesse público como o controlo de doenças e outras ameaças à saúde pública, realizar o tratamento dos dados pessoais dos empregados. A base legal referida no texto é o artigo 9.º, n.º 2.º, alíneas *c)* e *i*), apesar de parecer mais correto, no que concerne o tratamento de dados pelo empregador, a aplicação da autorização prevista na alínea *b*), que se refere especificamente ao cumprimento de obrigações da legislação laboral.

Outro ponto que merece especial atenção é o relativo aos riscos inerentes ao tratamento dos dados de localização, os quais, quando atrelados aos dados de saúde, podem permitir ao responsável pelo tratamento exercer grande controlo sobre os titulares dos dados. Este aspeto é de grande relevância por nos remeter aos cenários descritos na introdução, de constantes monitoramento e vigília sobre os cidadãos, podendo culminar com a quebra das resistências ao estabelecimento de uma sociedade da vigilância e, assim, atingir profundamente a autodeterminação informativa digital. Para essas situações, o Comité defendeu a aplicação da Diretiva Privacidade Eletrónica e ressaltou que, em princípio, os dados de localização somente podem ser utilizados pelo operador se forem tornados anónimos ou se for obtido o consentimento. Estas limitações, contudo, segundo o Comité,

podem ser superadas em caso de lei excecional que possa ser editada por algum Estado-membro com o objetivo de salvaguardar a segurança pública, tendo por fundamento o artigo 15.º da Diretiva Privacidade Eletrónica[63] [64].Por fim, destacou o Comité que os dados pessoais, no ambiente do combate à pandemia, podem ser tratados, mas desde que com finalidade específica e explícita, fornecendo, aos respetivos titulares, informações transparentes sobre as atividades de tratamento, as suas principais características, período de conservação dos dados e a finalidade. Recomenda a adoção de medidas de segurança adequadas e políticas de confidencialidade para evitar que os dados sejam divulgados a pessoas não autorizadas.

Extrai-se da referida Declaração a sinalização da preocupação do Comité quanto aos riscos que a pandemia fez recair sobre a proteção dos dados pessoais, enfatizando três vetores, sendo os de maior preocupação: o tratamento dos dados pelas autoridades públicas, o tratamento dos dados no ambiente de trabalho e o tratamento dos dados de localização para fins de rastreio.

O Comité procurou ressaltar os limites à atuação dos governos dos Estados-Membros impostos pela legislação de proteção de dados. Afirmou que os artigos 6.º e 9.º do RGPD e os princípios estabelecidos no Regulamento seriam bastantes para assegurar o devido respeito dos direitos dos titulares de dados. E, ao enfrentar a questão dos dados de localização, referiu-se ao artigo 15.º da Diretiva 2002/58/CE, de 12 de julho, que admite exceção às regras limitativas antes referidas e submete a disciplina da questão à lei nacional em situações de risco para a segurança.

A Declaração antecipa as principais questões que se anunciavam e indica os principais fundamentos para a defesa dos interesses e direitos dos titulares de dados pessoais, fazendo alusão aos artigos 6.º e 9.º do RGPD e salientando a possível aplicação do artigo 15.º da Diretiva 2002/58/CE, de 12 de julho.

---

63 A regra a que se refere o Comité está no c*aput* do artigo 15.º da Diretiva 2002/58/CE, de 12 de julho: "Artigo 1. Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.os. 1 a 4 do artigo 8.º e no artigo 9.º da presente Directiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas, tal como referido no n.º 1 do artigo 13.º da Directiva 95/46/CE. Para o efeito, os Estados-Membros podem designadamente adoptar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.ºs 1 e 2 do artigo 6.º do Tratado da União Europeia".

64 Para a interpretação do artigo 15.º da Diretiva, veja-se o acórdão do Tribunal de Justiça da União Europeia (TJUE) de 29 de janeiro de 2008, Productores de Música de España (Promusicae)/Telefónica de España SAU, C- 275/06, ECLI:EU:C:2008:54. Disponível em https://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06 10.01.2022.

Convém aqui examinar as situações destacadas na Declaração, em especial no que tange ao tratamento dos dados de saúde pelas autoridades, em vista ao direito à privacidade do cidadão, assim como no ponto relativo aos dados de localização, ou dados de tráfego, que se pretenderam utilizar para o rastreio de indivíduos. São pontos sensíveis relativamente à autodeterminação informativa no ambiente digital.

a) Tratamento de dados de saúde pelas autoridades públicas portuguesas com base no interesse público – Artigo 9.º, 2, *i)* do RGPD

O primeiro ponto relativo ao tratamento dos dados de saúde pelas autoridades públicas envolve vários aspetos, entre os quais a divulgação de informações nos relatórios e comunicados ao público em geral. O Estado deve atender ao princípio da transparência e publicidade, especialmente numa situação de crise sanitária, que lhe impõe prestar contas à sociedade das medidas adotadas para conter o aumento de casos, assim como dos resultados alcançados. Não foi por outro motivo que, em Portugal, a Autoridade Nacional de Saúde disponibilizou, sistematicamente, informações sobre o número de casos suspeitos de infeção, de casos confirmados, de recuperados e de óbitos. Informou, também, a distribuição desses casos pelo território português, apontando as regiões e os números da incidência, inclusive por concelho.

Alguns municípios portugueses divulgaram também os quantitativos e chegaram a informar dados por freguesia. Em alguns casos, deram a conhecer os dados de identificação e contatos de alguns infetados, nas suas páginas na *internet* ou redes sociais. Noutros casos, as informações dadas, apesar de anonimizadas, foram suficientes para conduzirem à identificação dos doentes, em situações verificadas em pequenas localidades, com poucos residentes.[65] São casos de evidente desrespeito ao sigilo que protege os dados pessoais de saúde.

É, pois, indubitável que os dados pessoais, inclusive os de saúde, podem ser objeto de tratamento pelas autoridades públicas.[66]

---

[65] A respeito desses casos, veja-se o relato da Comissão Nacional de Proteção de Dados- CNPD na orientação sobre divulgação de informações relativas a infetados por COVID-19. Disponível em https://www.cnpd.pt/media/4i4hmccv/orientacoes_divulgacao_informacao_infetados_covid-19.pdf 15.01.22

[66] É sempre bom lembrar que os *considerandos* prestam auxílio à interpretação do Regulamento, motivo pelo qual se deve atentar para o (46) que se refere aos tratamentos de dados que conciliam o interesse público e os interesses vitais "para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial situações de catástrofes naturais ou de origem humana", assim como o (54) que esclarece que "o tratamento de categorias especiais de dados pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados."

O tratamento dos dados pessoais é regulado, conforme conceito jurídico firmado no artigo 4.º, 2, do RGPD. Isso decorre do artigo 6.º, 1, alíneas c), d) e e) do RGPD, seja para cumprir uma obrigação jurídica[67], para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular ou para o exercício de funções de interesse público ou para o exercício de autoridade pública de que está investido o responsável pelo tratamento.[68]

Quanto aos dados especiais de saúde, além das hipóteses em que haja consentimento do respetivo titular, do que aqui não se cogita, a autorização do RGPD para o tratamento vem clara na alínea *i)* do inciso 2, do artigo 9.º do RGPD, que estabelece tal exceção à proibição genérica constante no inciso 1 desse mesmo artigo. Poder-se-ia considerar que o disposto na alínea *g*) também tivesse de ser aplicável, uma vez que é inegável a presença do interesse público. Porém, parece que a existência de um item específico destinado a tratar dos temas de saúde pública afasta a incidência de dispositivos mais genéricos. E é claro que "interesse público no domínio da saúde pública" se encaixa na perfeição na situação da pandemia, considerada como a prestação de cuidados de saúde e o acesso universal aos mesmos[69]. A referência, que o legislador faz a título de exemplo, a uma situação de "proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde" é mais do que suficiente para que se reconheça a aplicabilidade do inciso, uma vez caracterizado o interesse público ínsito a uma tal situação.

---

67 Melhor seria ter-se adotado a expressão 'obrigação legal', tal como se fez no artigo 7.º, c) da Diretiva 95/46/CE, de 24 de outubro de 1995, em que a mesma regra já constava. É que neste caso, a obrigação que pode justificar o tratamento é aquela decorrente de lei, pois a obrigação contratual já está contemplada na alínea b). Aliás, na versão do RGPD em inglês consta a expressão mais adequada – *legal obligation*; na versão em francês – *obligation légale*.

68 Segundo o que consta no Considerando (46) "O tratamento de dados pessoais também deverá ser considerado lícito quando for necessário à proteção de um interesse essencial à vida do titular dos dados ou de qualquer outra pessoa singular. Em princípio, o tratamento de dados pessoais com base no interesse vital de outra pessoa singular só pode ter lugar quando o tratamento não se puder basear manifestamente noutro fundamento jurídico. Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana."

69 O conceito jurídico de saúde pública encontra-se no Regulamento (CE) n.º 1338/2008 de 16 de Dezembro de 2008, relativo às estatísticas comunitárias sobre saúde pública e saúde e segurança no trabalho, no seu artigo 3.º/1, c) que assim a define: «Saúde pública», todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade.

A exigência que faz o RGPD é que o direito da União ou dos Estados-Membros prevejam medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional.

O sigilo profissional aí referido tem como destinatários os profissionais de saúde, sujeitos a essa regra jurídica e deontológica. Mas também o encarregado da proteção de dados está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o que dispõe o artigo 38.º, 5, do RGPD, assim como os responsáveis pelo tratamento de dados e todas as pessoas que intervenham em qualquer operação de tratamento de dados, os quais estão cobertos pelo dever de confidencialidade, de acordo com o artigo 10.º, 2, da Lei de Execução (LE). No que diz respeito aos dados de saúde, o legislador nacional foi além e estabeleceu regras que protegem o titular dos dados, impondo sigilo e confidencialidade àqueles que, por necessidade, participarem do tratamento desses dados. É o que se observa no artigo 29, incisos 1, 2, 3, 4 e 5.

Aliás, parece claro que o intuito do legislador português de atender à exigência de previsão de medidas – específicas e adequadas com vista à defesa dos direitos fundamentais e dos dados pessoais das pessoas singulares – posta na parte final do permissivo da alínea *i*) do inciso 2 do artigo 9.º do RGPD se expressou no artigo 29 da LE, que disciplinou conjuntamente o tratamento dos dados de saúde e genéticos.

Menezes Cordeiro,[70] defende que o disposto no artigo 29 não seria suficiente para atender às "exigências legais genéricas" do RGPD que alcançariam "*Identificação dos dados objeto do tratamento e fim em concreto prosseguido, previr medidas adequadas e específicas que salvaguardem os direitos e as liberdades do titular dos dados – direitos e deveres de informação, possibilidade de recorrer da decisão de tratamento, faculdade de acompanhar o processo de tratamento e, em particular, o sigilo profissional.*"

Diz ainda, no ponto, no mínimo sujeito a controvérsia: "Não *nos parece que o artigo 29.º da LE cumpra estas exigências legais: as medidas de salvaguarda aí previstas não podem ser descritas como sendo específicas. Nesse sentido e porquanto não sejam introduzidas medidas adicionais, não cremos que possam ser realizados tratamentos motivados pelo interesse público no domínio da saúde."*

Não parece ter razão o jurista. O artigo 29 da LE, mesmo não sendo um exemplo da boa técnica legislativa, é suficiente para tratar da confidencialidade e refere-se ao sigilo profissional, que, naturalmente, é tratado igualmente em outros diplomas nacionais que preexistiam ao RGPD, das quais destacam-se as Leis n.º 12/2005 de 26 de janeiro, que trata da informação genética pessoal e informação de saúde, e n.º 26/2016, de 22 de agosto, que aprova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos. São diplomas legais que, em complemento

[70] Cf. A. Barreto Menezes Cordeiro, *ob. cit*., p. 251

do artigo 29 da LE, atendem às exigências acima referidas, estabelecidas pela alínea *i*) do inciso 2, do artigo 9.º do RGPD. Inegavelmente, nessas leis se disciplinam o sigilo e a confidencialidade, impõem-se sanções a serem aplicadas em decorrência do seu incumprimento, regulamenta-se o direito de acesso do titular de dados, permitindo-lhe acompanhar o tratamento dos seus dados, formular reclamações e pedir a reforma das decisões, respeitada a estrutura administrativa existente no estado português.

Criou-se, inclusive, uma entidade administrativa independente, que funciona junto da Assembleia da República, a quem cabe zelar pelo cumprimento das disposições da referida lei, com funções disciplinares e decisórias: a Comissão de Acesso aos Documentos Administrativos – CADA.

Todo este arcabouço de leis e essa estrutura administrativa complexa servem o propósito, definido no RGPD, de viabilizar a concretização dos direitos assegurados aos titulares de dados. Além disso, não se pode deixar de destacar a Comissão Nacional de Proteção de Dados, uma entidade de controlo independente, prevista no capítulo VI do RGPD (artigos 51.º e seguintes), cuja organização e funcionamento são regulados pela Lei n.º 43/2004, de 18 de agosto, republicada como anexo à LE. A CNPD visa assegurar a execução do RGPD na ordem jurídica interna, controlando e fiscalizando-lhe o cumprimento, bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais.

A existência da entidade jurídico-administrativa anteriormente referida permite reconhecer a aplicabilidade do disposto na alínea i) do inciso 2 do artigo 9.º do RGPD quanto à possibilidade jurídica do tratamento de dados de saúde motivado pelo interesse público no domínio da saúde pública em Portugal.

Fixada esta premissa, convém destacar que a confidencialidade e o sigilo impostos sobre os dados de saúde, no RGPD ou na LE impedem a adoção da conduta das autarquias locais, relatada pela CNPD acima referida, de permitir a divulgação de dados pessoais dos infetados ou disponibilizar informações capazes de conduzir a essa identificação. É bom destacar que o tratamento dos dados em conformidade com o RGPD atrai a necessidade de atendimento aos princípios estabelecidos no artigo 5.º, *i*)[71] e inclusive ao da proporcionalidade.

Sobre a aplicação do princípio da proporcionalidade em relação à divulgação de dados pessoais para efeitos de transparência no setor público, o Grupo de Trabalho de Proteção de Dados do artigo 29.º da Diretiva 95/46/CE[72]

---

[71] Princípios da licitude, lealdade e transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade e responsabilidade.

[72] O grupo de trabalho foi criado ao abrigo do artigo 29.º da Diretiva 95/46/CE, constituindo-se num órgão consultivo independente europeu sobre a proteção de dados e a privacidade, cujas atribuições estão descritas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE.

pronunciou-se no Parecer n.º 02/2016[73]: "O princípio de proporcionalidade deve ser respeitado no decurso de cada operação de tratamento e, em especial, na fase de recolha dos dados e na sua eventual publicação subsequente". E acrescenta, ainda, que "a publicação em linha de informações que revelem aspetos irrelevantes da vida privada de uma pessoa singular não se justifica à luz dos princípios da equidade e da proporcionalidade". O parecer refere-se a decisões do TJUE nos processos apensos C-465/00, C-138/01 e 139/01, no sentido de que o tratamento de dados pessoais deve dar-se de forma proporcionada e, quanto à publicidade de dados pessoais, os órgãos jurisdicionais nacionais competentes devem «verificar se tal publicidade é, simultaneamente, necessária e proporcionada» ao objetivo prosseguido e apreciar se tal objetivo não poderia ter sido alcançado de forma igualmente eficaz por formas alternativas que fossem menos suscetíveis de afetar a privacidade das pessoas em causa.

A lição aplica-se à situação acima tratada, que envolveu divulgação de dados sensíveis de saúde pelas autoridades públicas portuguesas.

Patrícia Cardoso Dias [74] defende que se acrescente "*Aos princípios gerais vertidos no artigo 5.º a necessidade de qualquer tratamento de dados pessoais de saúde encontrar-se subsumido a uma base jurídica legitimadora nos termos do artigo 6.º coordenada com alguma das derrogações previstas no n.º 2 do artigo 9.º do RGPD para efeitos de licitude do tratamento de categorias de dados sensíveis.*

E sustenta, ainda, que "*As pessoas singulares devem, para cumprimento integral do conteúdo dos princípios vertidos no artigo 5.º, receber informações transparentes, redigidas em linguagem facilmente apreensível, em relação às operações de tratamento de dados pessoais e as suas principais caraterísticas, período de conservação e finalidades do tratamento. Os dados pessoais tratados devem ser objeto de medidas de segurança adequadas e políticas de confidencialidade que assegurem que não sejam divulgados a pessoas não autorizadas.*"

Parece correta a posição adotada. O atendimento a todos esses requisitos é, portanto, rigoroso para que se legitime o tratamento dos dados pessoais de saúde, com fundamento no artigo 9.º, 2, *i*) do RGPD.

b) Dados de localização e contato – plataforma Stayaway COVID – A experiência portuguesa

Um ponto abordado pelo Comité Europeu para a Proteção de Dados na declaração acima referida e que deve merecer especial atenção refere-se à utilização dos dados de telecomunicações como ferramenta de rastreio de pessoas infetadas. Na Declaração anteriormente referida, o Comité

[73] Parecer do Grupo de Trabalho de Proteção de Dados nº 02/2016 disponível em https://www.uc.pt/site/assets/files/475840/20160608_parecer_02_2016_publicacao_de_dados_pessoais_para_efeitos_de_tranparencia_no_setor_publico_wp239_pt.pdf 10.01.2022

[74] Cf. Patrícia Cardoso Dias, *ob. cit.*, p. 18.

manifestou-se no sentido de que "as medidas mais invasivas, como o «rastreio» de indivíduos (ou seja, o tratamento de dados históricos de localização não anonimizados), poderão ser consideradas proporcionais em determinadas circunstâncias e em função das modalidades concretas do tratamento dos dados." Portanto, deixou claro que, naquele momento, concordava com a possibilidade de se utilizarem desses meios de rastreio, não se pronunciando, entretanto, sobre se uma tal medida poderia ou não ser compulsória.

A utilização de *contact tracing systems*[75] *pode representar graves riscos à autodeterminação digital e tem potencial para gerar atitudes discriminatórias. A propósito desta questão essencial, veja-se o pronunciamento da Organização Mundial de Saúde* [76] *em que, após destacar as possíveis vantagens de se utilizar a tecnologia em prol do combate à pandemia, adverte, com razão: "Yet such uses of data may also threaten fundamental human rights and liberties during and after the COVID-19 pandemic. Surveillance can quickly traverse the blurred line between disease surveillance and population surveillance. Thus, there is a need for laws, policies and oversight mechanisms to place strict limits on the use of digital proximity tracking technologies and on any research that uses the data generated by such technologies*."

O tema veio a ser tratado, em Portugal, no Decreto-Lei n.º 52/2020 de 11 de agosto que definiu o responsável pelo tratamento dos dados e regulou a intervenção do médico no sistema Stayaway Covid. Tratava-se, em poucas palavras, de aplicação capaz de armazenar dados de contato, e notificar aos portadores de aparelho telemóvel em que essa aplicação estivesse instalada, sobre situação capaz de representar risco de contágio, pela proximidade ocorrida em relação a outro aparelho em que tenha sido inserido código representativo de infeção do seu portador pelo vírus da COVID-19.

O referido Decreto-Lei estabeleceu, no artigo 2.º, que tal aplicação deveria "respeitar a legislação europeia e nacional aplicável à proteção de dados pessoais, nomeadamente o Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, a Lei n.º 58/2019, de 8 de agosto, e demais legislação aplicável".

O Decreto-Lei fez referência expressa às "Diretrizes n.º 4/2020, do Comité Europeu para a Proteção de Dados, sobre a utilização de dados de localização e meios de rastreio de contactos no contexto", nas quais o Comité

---

75 De acordo com a OMS, *"contact tracing is the process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission. When systematically applied, contact tracing will break the chains of transmission of an infectious disease and is thus an essential public health tool for controlling infectious disease outbreaks".* Em Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing, Interim guidance, de 28.05.2020: Disponível em https://www.who.int/publications/i/item/WHO-2019-nCov-Ethics_Contact_tracing_apps-2020.1 06.062022

76 *ob. cit., p.6*

se manifestara do seguinte modo: "o CEPD já tomou posição sobre o facto de a utilização de aplicações de rastreio de contactos dever ser voluntária e não dever depender do rastreio de movimentos individuais, mas sim de informações sobre a proximidade dos utilizadores".[77]

É de estranhar que o Governo de Portugal, adotando posição divergente da que fora manifestada no Decreto-Lei 52/2020, uma vez que ali se colhera a manifestação do EDPB (*European Data Protection Board*) no sentido de a utilização da aplicação dever ser voluntária, apresentou uma proposta de Lei (n.º 62/XIV/2ª GOV) na qual se previa, além de outras medidas, a utilização compulsória da tecnologia.[78] No artigo 4.º da referida proposta, determinava-se a "obrigatoriedade da utilização da aplicação Stayaway Covid em contexto laboral ou equiparado, escolar e académico", "em especial os trabalhadores em funções públicas, funcionários e agentes da Administração Pública, incluindo o setor empresarial do Estado, regional e local, profissionais das Forças Armadas e de forças de segurança." A proposta criava o dever de o utilizador "proceder à inserção na aplicação do código de legitimação pseudoaleatório, que deve figurar do relatório que contenha o resultado do teste laboratorial de diagnóstico".

A Ordem dos Advogados de Portugal, ouvida, opôs-se à referida proposta por fundamentos jurídicos relevantes (artigos 32.º, n.º 8,10 e 34.º, n.º4 da Constituição).[79]

---

[77] A íntegra das Diretrizes do CEPD está disponível em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf 06.06.2022. Destaca-se que, não obstante firmar a premissa de que a utilização da aplicação exigia o consentimento do titular de dados, o Comité acrescentou: "No entanto, são permitidas derrogações dos direitos e das obrigações previstas na diretiva nos termos do artigo 15.º, sempre que as mesmas constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para alcançar determinados objetivos

[78] Em 15.10.2020, o Diário de Notícias *online* informava sobre uma proposta de lei do governo que previa multas de até 500 euros para quem não tivesse a app Stayaway Covid. A fiscalização do cumprimento da obrigação competiria à Guarda Nacional Republicana, à Polícia de Segurança Pública, à Polícia Marítima e às polícias municipais. Disponível em https://www.dn.pt/pais/lei-propoe-multas-ate-500-euros-para-falhas-no-uso-de-mascara-e-stayaway-covid-12922740.html 06.06.2022

[79] Cf. O seguinte trecho do parecer da Ordem dos Advogados de Portugal sobre a referida proposta de lei: "No caso concreto, a restrição que o Governo pretende impor através da consagração da obrigatoriedade da aplicação ao direito da reserva da intimidade da vida privada e familiar, ao direito à inviolabilidade dos meios de comunicação privada e à proibição da utilização da informática para tratamento de dados referentes à vida privada, não é claramente adequada (por não ser eficaz para prevenir e deter a epidemia, uma vez que só poderá ser utilizada pelos cidadãos que sejam portadores de equipamento compatível com a aplicação), não é exigível (porque o legislador dispõe de outros meios menos restritivos para alcançar o mesmo fim) e é excessiva e desproporcional. A par disso, a CRP proíbe a ingerência das autoridades públicas nas telecomunicações, sendo nulas todas as provas obtidas mediante abusiva intromissão na vida privada, no domicílio ou nas telecomunicações, aplicando-se essa proibição ao processo contra-ordenacional, o que, no caso concreto, impossibilitaria o sancionamento dos utilizadores com a aplicação de coima (cf. Artigos 32.º, n.º8, 10 e 34.º, nº. 4)."

Especial destaque merece a posição adotada pela Comissão Nacional de Proteção de Dados – CNPD que, em fundamentado parecer de 27.10.2020 (parecer 2020/129)[80], destacou, inicialmente, a tensão existente, naquele momento, entre o direito à vida e à saúde e o direito à privacidade[81]: "*A CNPD compreende a necessidade de definição de medidas adequadas a acautelar o interesse público de saúde pública e a salvaguardar os direitos fundamentais à vida e à integridade física, os quais podem implicar restrições de outros direitos fundamentais, como o direito à liberdade e à privacidade. Não pode deixar de sublinhar, contudo, que tais restrições têm de refletir um equilíbrio entre os diferentes direitos e valores constitucionalmente protegidos, não podendo ultrapassar o limite último do respeito pelo conteúdo essencial dos direitos, liberdades e garantias, no quadro do Estado de Direito democrático em que nos movemos*."

Feita esta introdução ao tema, a Comissão prosseguiu, esclarecendo que a aplicação em questão (Stayaway Covid) assentava num sistema descentralizado de tratamento de dados, o que significava que os dados de contato ficavam armazenados no próprio aparelho e pseudonimizados[82] "uma vez que permitem, por relacionamento com outra informação, identificar a pessoas a que dizem respeito".

E com base em informações técnicas, relativas ao funcionamento da aplicação, concluiu que "*A Google e a Aple criaram uma interface (GAEN) para habilitar o funcionamento de aplicações de rastreamento de proximidade, disponibilizando o acesso a funcionalidades ao nível do sistema operativo do dispositivo móvel, como sejam o acesso à componente Bluetooth, a geração de chaves de identificadores pseudoaleatórios e o seu cruzamento para cálculo do risco, as quais não são executadas pela aplicação. Com isto, uma parte substancial do tratamento de dados não é controlada pelo responsável pelo tratamento (a Direção-Geral de Saúde), mas, sim, por uma parceria de duas das maiores empresas privadas de tecnologia. Esta é também uma das razões porque a utilização da aplicação só foi considerada legítima no ordenamento jurídico nacional se dependesse exclusivamente da vontade dos cidadãos a*

---

[80] O parecer é é intitulado – Parecer sobre a obrigatoriedade do uso de máscara para acesso ou permanência nos espaços e vias públicas e a obrigatoriedade de utilização da aplicação Stayaway Covid. Disponível em https://www.cnpd.pt/covid-19/ 23.01.2022.

[81] Para Paulo Mota Pinto, a privacidade se baseia numa *tensão entre o social e o individual*. *Ob. Cit*. p. 509.

[82] Cf. A. Barreto Menezes Cordeiro, *ob*. cit. p. 149: "A pseudonimização consiste, nos termos do artigo 4.º, 5), (i) num tratamento efetuado sobre dados pessoais (ii) que impossibilita a identificação do titular de determinados dados, sem a utilização da informação suplementar. A estes dois critérios estruturais acresce um (iii): a informação suplementar deve ser conservada separadamente, de forma a impedir a identificação do titular dos dados. (…) A pseudonimização incentivada pelo legislador, permitir reduzir os riscos de divulgação da identidade do titular dos dados pessoais, acautelando os seus interesses, e facilitar o cumprimento, pelos responsáveis pelo tratamento ou pelo subcontratante, dos deveres impostos pelo RGPD."

sua utilização, o mesmo se aplicando à introdução do código de legitimação, que desencadeia o alerta de risco de contágio junto dos utilizadores da aplicação e que tenham ficado registados como tendo estado próximos do utilizador que é portador do vírus."

Em seguida, a Comissão asseverou que "pelo menos quanto aos dispositivos Android, a interface GAEN implica a recolha permanente do dado 'localização', uma vez que deixa de ficar ao critério de cada um poder desativar essa funcionalidade se e quando o desejar, permitindo à Google rastrear as deslocações e movimentos dos cidadãos utilizadores desta aplicação para outras finalidades".

Além disso, e com razão, a Comissão considerou que a imposição das obrigações concernentes à utilização da aplicação geraria impacto nos direitos fundamentais à liberdade, à reserva ou respeito pela vida privada, à inviolabilidade das comunicações eletrónicas e à proteção dos dados pessoais (artigos 26.º, 27.º, 34.º, e 35.º da CRP e artigos. 6.º, 7.º e 8.º da CDFUE), direitos que somente poderiam ser afetados excecionalmente, desde que respeitado o princípio da proporcionalidade (adequação, necessidade e caráter não excessivo da restrição) e sem afetar o conteúdo essencial dos direitos (artigo 18.º, n.os 2 e 3, e artigo 52.º, n.º 1 da CRP).

A Comissão mostrou-se francamente contrária à proposta. E tinha toda a razão em assim se posicionar, pois, a medida, se aprovada, representaria uma violação grave dos direitos fundamentais dos cidadãos, absolutamente desproporcionada e afrontaria o artigo 18.º, 2, da CRP e o artigo 5.º, 1, do RGPD. A imposição, ainda que por lei, da utilização de tecnologia de compartilhamento de dados pessoais de localização estaria próxima dos piores cenários temidos no texto de Harari, citado no início deste estudo.

Não se trata somente de uma violação das regras de proteção de dados (o que já seria bastante para rejeitar a proposta); a intenção do Governo era de que o cidadão se submetesse a uma série de obrigações que violavam por completo a sua liberdade. Estaria obrigado a instalar a aplicação (se compatível com o seu aparelho) e, diante de uma fiscalização (por agentes de segurança), seria obrigado a desbloquear o aparelho, permitir ao agente a verificação de pelo menos o seguinte: (i) da compatibilidade do aparelho com a aplicação; (ii) do descarregamento da aplicação; (iii) da ativação do *Bluetooth*.

A compulsoriedade de que se reveste a medida, como se vê, não é somente quanto ao fornecimento da informação pessoal à autoridade (e, quiçá, ao terceiro com quem o titular dos dados possa ter tido contato)[83], mas envolve uma série de condutas por parte do cidadão, titular dos dados, que representa

[83] É natural que, em muitas situações, por serem poucos os contatos pessoais, especialmente em tempos de pandemia, seja possível identificar-se aquela pessoa que, preenchendo as características exigidas para acionar o alarme de risco de contágio (proximidade por determinado período de tempo), seja o provável infetado. Se não houvesse outros defeitos, este, por si só, já importaria em quebra da obrigação de confidencialidade.

uma devassa na sua vida privada, uma exposição da sua intimidade, podendo resultar na autoincriminação, constituindo absurdos inaceitáveis, que mostram quão desproporcionada é a proposta.

Nem tudo se permite, mesmo com o objetivo de atender aos interesses maiores da saúde pública. Segundo Alice Donald e Philip Leach [84]: *If a state takes far-reaching steps to protect life and health, it is highly likely that this will result in the restriction of other rights. However, as Mavronicola explains, while the pandemic may justify or even require exceptional emergency measures, it does not give carte blanche to states to take actions that are impermissible under international human rights law*. [85]

A proposta lei n.º 62/XIV/2ª GOV não foi adiante e a aplicação foi admitida em Portugal, com base no DL 52/2020, de 11 de agosto, dependente de um ato voluntário, de consentimento do titular de dados. A rejeição da proposta, em função da resistência que encontrou na sociedade, em especial nos órgãos que se dedicam à proteção dos dados pessoais, representa a prevalência do direito e, neste caso, revela que o ordenamento jurídico foi eficaz na prevenção contra o arbítrio.

4. O CERTIFICADO DIGITAL COVID DA UE – CRIAÇÃO, FINALIDADE, TRATAMENTO LEGAL

Com o objetivo de combater a propagação do vírus SARS-COV-2, os países adotaram, com base no princípio da precaução, medidas de isolamento, cada qual com um determinado nível de restrições, que tiveram grande impacto na liberdade e especialmente no direito de livre circulação. Foram impostas restrições severas a locomoção, viagens transfronteiriças, exigindo-se o cumprimento de medidas de quarentena, isolamento e realização de testes para despistagem da infeção.[86] [87]

---

[84] Alice Donald E Phillipe Leach –Human Rights – The Essential Frame of Reference in the Global Response to COVID-19. Disponível em https://verfassungsblog.de/humanrights-the-essential-frame-of-reference-in-the-global-response-to-covid-19/ 13.06.2022

[85] No mesmo artigo, os autores concluem: "*In other respects, too, measures adopted by states which comply with a human rights framework are likely to be more effective in protecting life and health, than ones that restrict other rights disproportionately. For example, voluntary contact tracing apps (installed onto smart phones) which rely on a critical mass of public uptake will not be effective if there are concerns about a disproportionate invasion of privacy*".

[86] Na União Europeia, foi adotada a Recomendação (UE) 2020/1475 de 13 de outubro de 2020 sobre uma abordagem coordenada das restrições à liberdade de circulação em resposta à pandemia de COVID-19, com critérios a serem adotados pelos Estados-Membros para evitar a discriminação e para alcançar, tanto quanto possível, uma ação harmoniosa no tema da circulação no território europeu.

[87] Para um relatório detalhado sobre as medidas de restrição impostas por diversos países nos primeiros meses da pandemia, incluindo medidas de limitação à imigração e supressão de direitos humanos, consulte-se Verfassungsblog symposium organizado por

Essas medidas, além de implicarem graves restrições ao direito de livre circulação, dentro e fora dos países, acarretavam uma enorme perda económica, com especial ênfase nos campos do turismo e transportes.

Com o advento das vacinas contra o SARS-COV-2, a verificação da sua eficácia na produção de resposta imunológica e, consequentemente, na produção de resultados positivos para auxílio no objetivo de contenção da pandemia, passou-se a considerar fortemente a hipótese de se voltar a permitir a livre circulação de pessoas imunizadas, que se mostraram menos propensas a transmitir a doença. Neste conjunto ideal de pessoas, e de acordo com dados científicos, incluem-se os vacinados, dentro do prazo de eficácia da vacina, assim como os que obtiveram um resultado negativo em teste de despistagem à COVID-19, bem como as pessoas que recuperaram da doença nos seis meses anteriores.

Foi considerado que a livre circulação de tais pessoas não representava risco significativo para a saúde pública, motivo pelo qual as restrições em relação a esse grupo específico poderiam ser afastadas, ainda que temporariamente, pois o objetivo das limitações era, exatamente, impedir a propagação do vírus, que não ocorreria, significativamente, com a circulação de pessoas alegadamente imunes.

Muitos países começaram a adotar medidas tendentes à criação de documentos capazes de atestar essa situação, fosse em relação à vacinação, fosse em relação à recuperação ou testagem, o que originou a ideia de se emitirem certificados com tais informações, que rapidamente viriam a ser denominados certificados de vacinação.

No âmbito da União Europeia, tais certificados de vacinação possibilitariam a retoma da livre-circulação entre países, ajudando a reativação da economia. Para isso, os certificados teriam que ser interoperáveis, compatíveis, seguros e verificáveis, de forma a que pudessem ser reconhecidos e utilizados por todos os Estados-membros, assim como pelas empresas de transporte e demais agentes económicos envolvidos. Era necessária uma abordagem uniforme da questão, para evitar que cada Estado-membro criasse o seu certificado, o que dificultaria a aceitação em todo o território da União.

Ficou decidido, então, que seria estabelecido um regime comum para a emissão, verificação e aceitação pelos Estados-membros, de certificados interoperáveis de vacinação, teste e recuperação da COVID-19 (Certificado Digital COVID da UE[88]), em formato digital ou em papel (ou em ambos).

Como a questão envolvia o tratamento de dados especiais de saúde em larguíssima escala, foram ouvidos a Autoridade Europeia para a Proteção de Dados e o Comité Europeu para a Proteção de Dados, nos termos do artigo 42.º do Regulamento (UE) 2018/1725. Essas entidades emitiram um parecer

Joelle Grogan Disponível em https://intr2dok.vifa-recht.de/receive/mir_mods_00008563 . 13.06.2022.

88 Também conhecido como Certificado Verde Digital.

conjunto em 31 de março de 2021. [89] Em 14 de junho de 2021, foi editado o Regulamento (EU) 2021/953, cujo objeto era o estabelecimento de um regime para a emissão, verificação e aceitação de certificados interoperáveis de vacinação, teste e recuperação da COVID-19 («Certificado Digital COVID da UE»), para facilitar o exercício do direito de livre circulação dos seus titulares durante a pandemia e contribuir, também, para facilitar o levantamento gradual das restrições à livre circulação adotadas pelos Estados-membros, em conformidade com o direito da União, para limitar a propagação do SARS-CoV-2, de forma coordenada (art. 1.º).

4.1. QUESTÕES POLÉMICAS E RISCOS PARA A AUTODETERMINAÇÃO DIGITAL

O tema do Certificado Digital COVID da UE envolve um debate intenso sobre questões ético-jurídicas, muitas das quais estão além dos limites do presente estudo. Isso decorre, desde logo, das consequências de se adotar o Certificado como passaporte para a retoma da livre-circulação.

No próprio parecer conjunto EDPB/EDPS acima referido, há menção expressa a essa situação, com especial ênfase para a manifestação da Organização Mundial da Saúde (OMS), no seu «*Interim position paper: considerations regarding proof of COVID-19 vaccination for international travellers*», de 5 de fevereiro de 2021, em que declarou: "(...) as autoridades nacionais e os operadores de transporte não devem introduzir requisitos de prova de vacinação contra a COVID-19 aplicáveis às viagens internacionais como condição para a partida ou para a entrada, dado que ainda existem incógnitas críticas a respeito da eficácia da vacinação na redução da transmissão".

O parecer conjunto EDPB/EDPS também mencionava o estudo desenvolvido pelo Instituto Ada Lovelace, intitulado "*What place should COVID-19 vaccine passports have in society*?".[90] Neste estudo leem-se as conclusões de pesquisas sobre o tema da adoção da vacinação contra a COVID-19 como elemento para discriminação entre pessoas, com o objetivo de imposição de limitações mais severas à liberdade individual, considerado o alegado risco de transmissão do vírus. O trabalho do Instituto Ada Lovelace foi desenvolvido por *experts* nas áreas de imunologia, epidemiologia, sociologia, desenvolvimento internacional, direito, história da medicina, saúde pública, ética e *design* de sistemas. De entre as conclusões a que chegou o grupo multidisciplinar, destaca-se a seguinte: *"At present, vaccination status does not offer clear or conclusive evidence about any individual's risk to others via*

---

[89] Joint Opinion EDPB and EDPS 04/2021 na versão em língua portuguesa, disponível em https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042021-proposal_pt 10.01.2022.

[90] AD ALOVELACE INSTITUTE – What place should COVID-19 vaccine passports have in society? Findings from a rapid expert deliberation chaired by Professor Sir JONATHAN MONTGOMERY**.** Disponível em https://www.adalovelaceinstitute.org/summary/covid-19-vaccine-passports/ 12.04.2022

transmission, so cannot be a robust basis for risk-based decision making, and therefore any roll-out of a digital passport is not currently justified".

O próprio parecer conjunto destaca esse ponto, no seu item 14, quando assevera: "A este respeito, observamos que, no momento da elaboração do presente parecer conjunto, parecem existir poucos dados científicos que corroborem o facto de que a toma de uma vacina contra a COVID-19 (ou a recuperação da COVID-19) conceda imunidade e a duração dessa imunidade". O parecer data de 31 de março de 2021[91].

É este o primeiro ponto da marcante polémica gerada com a utilização do certificado vacinal como elemento de discriminação de pessoas não vacinadas (e não submetidas ao teste ou recuperadas da doença). A base ético-jurídica para o estabelecimento do discrímen pressupunha que se estabelecesse, solidamente, a premissa de que aqueles vacinados seriam incapazes de transmitir o vírus; ao contrário, não se poderia justificar o tratamento diferenciado.

Este tema tem óbvia relação com a proteção de dados, uma vez que o certificado digital não é outra coisa senão um repositório de dados pessoais de saúde, armazenados digitalmente ou em papel. A necessidade de se exibir um conjunto desses dados como condição para se obter maior liberdade, numa sociedade moderna, envolve claramente a autodeterminação informativa, que se define, relativamente a cada pessoa, como "o direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em «simples objeto de informação»" na feliz expressão de Gomes Canotilho e Vital Moreira.[92]

Em qualquer situação que envolva um tratamento diferenciado entre cidadãos da UE, ainda que respaldada no interesse público, deve-se sempre ter em mente o princípio da proporcionalidade e o que dispõe o artigo 52.º da CDFUE: "*Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efectivamente a objectivos de interesse geral reconhecidos pela União, ou à necessidade de protecção dos direitos e liberdades de terceiros."*

---

[91] Sobre o tema da propagação do vírus pelos vacinados, Andrew Lee, no *site The Conversation* disponível em https://theconversation.com/faroe-islands-superspreader-event-why-transmission-among-the-triple-vaxxed-shouldnt-alarm-you-174301, acedido em 06.06.2022, afirma: *"There is now ample evidence that shows the vaccines are not very effective at stopping a vaccinated person from getting infected or from spreading infection. This was graphically illustrated by a superspreading event that took place in the Faroe Islands where 21 out of 33 triple-vaccinated healthcare workers who attended a private gathering caught omicron. This was also despite the fact that several had done a PCR or lateral flow test in the 36 hours before the event".*

[92] Cf. Gomes Canotilho e Vital Moreira, *ob. cit*. p. 557.

Especificamente sobre essa questão, Oskar Josef Gstrein, Andrej Zwitter e Dimitry Kochenov[93] chegam a referir uma "onda de *apartheid*" a ser evitada, destacando que a questão do passaporte vacinal não envolve tantos problemas técnicos (*privacy by design*) mas, sim, questões sociais, de integração: *"the technical design to make vaccination passports 'private by design', secure and usable are relatively minor. (…) Ultimately, what counts is not the technical fix, but the implementation in society. There is no way to hack oneself out of this pandemic. In order to avoid that the next wave of the COVID-19 pandemic will be the 'wave of apartheid', we need thoughtful, feasible and practical solutions that are widely accessible and work for everyone*".[94]

A implantação do passaporte vacinal, conjugada com a paulatina liberação de algumas atividades para os portadores, e só para eles, pela pluralidade de situações que envolve, é capaz de gerar polémicas infindáveis, além de lançar os não vacinados em situação de inegável prejuízo no que concerne as suas liberdades. A medida pode ter a sua proporcionalidade em relação ao objetivo de interesse público prosseguido posta em causa, tendo em vista o princípio da dignidade da pessoa humana, assim como diante da incerteza quanto à sua efetividade.

4.2. DESVIO DA FINALIDADE DETERMINADA – A UTILIZAÇÃO DO CERTIFICADO DIGITAL PELOS ESTADOS-MEMBROS PARA OBJETIVOS NÃO PREVISTOS NO REGULAMENTO (UE) 2021/953 DE 14 DE JUNHO DE 2021

O Certificado Digital, como já destacado, foi concebido para garantir o direito fundamental de livre circulação, especialmente no território dos Estados-Membros da União Europeia, e superar as restrições à entrada ou a exigência, para os viajantes transfronteiriços, de cumprimento de autoisolamento ou testagem para despistagem da infeção por SARS-CoV-2.

A sua criação decorreu do facto de, naquele momento (primeiro semestre de 2021), muitos Estados-Membros terem lançado ou manifestado intenção de lançar iniciativas para a emissão de certificados de vacinação, cumprindo à União regulamentar e uniformizar a medida, com o objetivo de impedir perturbações significativas no exercício do direito de livre circulação

---

93 Cf. Oskar Josef Gstrein, Andrerj Zwitter e Dimitry Kochenov – A Terrible Great Idea? COVID-19 'Vaccination Passports' in the Spotlight, Disponível em https://www.compas.ox.ac.uk/2021/a-terrible-great-idea-covid-19-vaccination-passports-in-the-spotlight/ 09.05.2022

94 Considerem-se, também, neste contexto, as seguintes advertências de Steven Greenberg, no artigo "I'm triple-vaxxed. The Green Pass system is bankrupt. The system marginalizes and publicly humiliates the unvaccinated, punishing rather than reforming, and creating even greater rifts in Israeli society" Disponível em https://blogs.timesofisrael.com/im-triple-vaxxed-the-green-pass-system-is-bankrupt/ : "*The unvaxxed will continue to live and work among us. They will continue to be our neighbours, parents in the schools our children attend, shoppers in the supermarkets we frequent. Demonization and public humiliation of the unvaxxed serve nothing but the most base of our instincts"*. 05.07.2022

que pudessem ser causadas pelos Estados-Membros, em iniciativas unilaterais capazes de prejudicar o bom funcionamento do mercado interno, nomeadamente do turismo.

Foi esse o intuito declarado do legislador da União ao adotar o Regulamento (UE) 2021/953 de 14 de junho de 2021 relativo a um regime para a emissão, verificação e aceitação de certificados interoperáveis de vacinação, teste e recuperação da COVID-19 (Certificado Digital COVID da UE), a fim de facilitar a livre circulação durante a pandemia de COVID-19. [95]

O artigo 10.º, 2, do Regulamento é claro sobre a finalidade para a qual os dados pessoais são inseridos no Certificado: "*Para efeitos do presente regulamento, os dados pessoais contidos nos certificados emitidos nos termos do presente regulamento são tratados apenas para efeitos de acesso e verificação das informações constantes do certificado, a fim de facilitar o exercício do direito de livre circulação na União durante a pandemia de COVID-19.*"

Interessante notar que o Regulamento 2021/953 reconhece que o RGPD é aplicável ao tratamento de dados necessário para a emissão, verificação e aceitação do Certificado Digital e estabelece como fundamento jurídico para o tratamento, além do artigo 6.º, n.º 1, alínea *c*), do RGPD, o artigo 9.º, 2, alínea *g*) daquele Regulamento. Este aspeto demonstra que a finalidade ali declarada não é a da alínea *i*), como parece, à primeira vista, ser a mais apropriada. O interesse público, em questão, a partir dessa premissa fixada pelo Regulamento, seria permitir a livre circulação mais do que algum interesse público no domínio da saúde pública.

Como decorre do artigo 9.º, 2, alínea *g*), do RGPD, o tratamento desses dados deve: *i*) respeitar o princípio da proporcionalidade diante do objeto visado; *ii*) respeitar a essência do direito à proteção de dados pessoais; iii) prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados.[96]

Segundo MENEZES CORDEIRO, respeitar a essência do direito à proteção de dados significa que "do tratamento não pode resultar um total esvaziamento da intrínseca relação pessoal e individual existente entre os dados tratados e o seu titular."[97] Isto importa em que qualquer limitação à privacidade deva dar-se no limite do necessário[98], fazendo-se a ponderação equilibrada dos

---

[95] Veja-se, a este respeito, o considerando n.º 12: "A fim de facilitar o exercício do direito de livre circulação e residência no território dos Estados-Membros, deverá ser estabelecido um regime comum para a emissão, verificação e aceitação de certificados interoperáveis de vacinação, teste e recuperação da COVID-19 (Certificado Digital COVID da UE)".

[96] Destaque-se o facto de que a alínea *g*) não contém qualquer referência ao sigilo profissional, diferentemente do que acontece com a alínea *i*) do mencionado dispositivo.

[97] Cf. A. Barreto Menezes Cordeiro *Ob. cit.* p. 249

[98] TJUE, acórdão Schecke, processos apensos C-92/09 e C-93/09, item 77: "as derrogações à protecção dos dados pessoais e as suas limitações devem ocorrer na estrita medida do necessário".

interesses em questão, sendo que tal não pode ir ao ponto de atingir os elementos essenciais do direito subjetivo à proteção de dados.

Porém, como se constatou logo em seguida, a finalidade para a qual foi concebido o Certificado e que é a justificativa para o tratamento dos dados pessoais nele contidos acabou por ser alargada indevidamente pelos Estados-Membros, criando-se uma situação de facto em que a exposição dos dados sensíveis de saúde passou a ser necessária como condição para o exercício de outros direitos, não apenas de livre circulação, o que levou a que esses dados fossem objeto de generalizada exposição e consulta.

É bom destacar que a consulta aos dados, por si só, caracteriza tratamento, conforme o artigo 4.º, 2, do RGPD.

Tal situação, em que os dados sensíveis de saúde são tornados públicos, como requisito para praticamente toda e qualquer atividade social, desde o comparecimento em festas, a frequência em restaurantes ou salas de espetáculo, inegavelmente representa o esvaziamento completo do direito à proteção desses dados, à autodeterminação informativa. É clara a violação ao próprio artigo 9.º, 2, alínea *g*) do RGPD, em que se fundamenta o Regulamento 2021/953, de 14 de junho de 2021. Mais ainda se há de considerar ilegal a situação ao ter como fundamento legal do tratamento a alínea *i*), do mencionado inciso, que parece ser a pertinente. Isto porque tal alínea menciona expressamente o sigilo profissional que estaria impossibilitado numa situação destas, de ampla exposição dos dados de saúde.

O Parecer Conjunto EDPB/EDPS acima referido já manifestava o receio de que os certificados tivessem a sua destinação indevidamente expandida pelos Estados-Membros, para além dos limites objetivos declarados pela União, de permitir a livre-circulação. O seguinte trecho do parecer é indicativo desse risco que já então se antecipava: "*O CEPD e a AEPD consideram que, dado o caráter da ingerência das medidas apresentadas pela proposta, qualquer outra eventual utilização do quadro e do Certificado Verde Digital com base no direito dos Estados-Membros, outra que não a facilitação do direito de livre circulação entre os Estados-Membros da UE, não é abrangida pelo âmbito de aplicação da proposta nem se insere, por conseguinte, no parecer conjunto do CEPD e da AEPD. Não obstante, o CEPD e a AEPD consideram que se os Estados-Membros persistirem na implementação do Certificado Verde Digital com base no direito dos Estados-Membros para qualquer outra eventual utilização que não a utilização prevista de facilitar a livre circulação entre os Estados- Membros da UE, tal poderá acarretar consequências e riscos indesejados para os direitos fundamentais dos cidadãos da UE.*"

No mesmo parecer, advertia-se: "*Ao abrigo de uma base jurídica nacional, qualquer outra utilização do Certificado Verde Digital e do quadro conexo não*

deveria ser suscetível, jurídica ou factualmente, de comportar discriminação baseada em ter (ou não) sido vacinado ou ter recuperado da COVID-19".[99]

Já era expectável que os Estados-Membros pudessem pretender criar legislações nacionais que autorizassem a utilização do Certificado Digital como um requisito de facto para a prática de atividades triviais, como acesso a bares e restaurantes, salas de espetáculos, cultos, lojas, ginásios, e outras atividades assemelhadas, e assim tentar impulsionar as próprias economias, aliviando os seus cidadãos das restrições decorrentes da pandemia. Tal alívio, entretanto, não seria extensível a todos, senão aos que tivessem consigo os certificados digitais, repletos de dados sensíveis, verdadeiras insígnias sem as quais não se abriam as portas para o 'novo normal'.

Porém, tal medida, é impossível negar, representaria um avanço sobre os limites da finalidade declarada na criação do Certificado e traria, segundo o parecer, "riscos indesejados para os direitos fundamentais dos cidadãos da UE". Em outras palavras, poderia representar o que Gstrein, Zwitter e Kochenov chamaram "*wave of apartheid*".

Em Portugal, o Decreto-Lei n.º 54-A/2021, de 25 de junho, cujo objeto era executar, na ordem jurídica interna, o Regulamento (EU) 2021/953, logo no seu introito, revelou o desvio da finalidade. Com efeito, no Decreto-Lei, prevê-se que os Certificados Digitais possam ser utilizados, para além dos fins previstos no Regulamento, também "*em matéria de acesso a eventos de natureza cultural, desportiva, corporativa ou familiar*."[100] Nenhuma dessas finalidades se encontra prevista ou autorizada no Regulamento 2021/953 de 14 de junho de 2021.

Deve ser enfatizado que nem mesmo se cuidou de incluir, no Decreto-Lei, com base no artigo 4.º, 2, *g*) do RGPD, disposições específicas sobre as categorias de entidades que pudessem proceder à verificação do certificado, e nem se previram garantias para os titulares de dados com o objetivo de se evitarem os abusos, como reputavam necessário tanto o CEPD como a AEPD no parecer conjunto anteriormente mencionado.

Repise-se que o simples ato de consulta aos dados constantes no Certificado Digital já representa tratamento e não há um regime jurídico que garanta aos titulares de dados o respeito ao sigilo que é devido por parte daqueles que

---

[99] O parecer conjunto menciona ainda que "a inclusão de tal base jurídica no direito dos Estados-Membros deve, no mínimo, incluir disposições específicas que identifiquem claramente o âmbito e a extensão do tratamento, a finalidade específica subjacente, as categorias de entidades que podem proceder à verificação do certificado, bem como as garantias relevantes para evitar o abuso, tendo em conta os riscos para os direitos e as liberdades dos titulares dos dados."

[100] O *site* do Diário da República eletrónico em que é publicado o DL, na parte relativa ao resumo em linguagem clara (sem valor legal), contém o seguinte: "este decreto-lei permite que quem tenha um Certificado Digital COVID da UE não fique sujeito a restrições em matéria de viagens aéreas e marítimas com destino a Portugal, em matéria de circulação pelo território nacional e em matéria de acesso a determinados eventos."

tenham contato com o Certificado, conforme exigido na alínea *i*) do n.º 2 do artigo 9.º do RGPD.[101]

Além disso, a submissão dos dados sensíveis de saúde à exposição generalizada, para os fins mais comezinhos e triviais, reverte na completa aniquilação da privacidade que deve permear o tratamento desses dados.

Diante de um cenário com tais características, que a reação dos Estados à pandemia acabou por criar, é mesmo difícil cogitar a previsão de medidas "adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados". É irrecusável o atentado que se comete contra a autodeterminação informativa digital, pois os titulares dos dados, em tal situação, não exercem qualquer controlo sobre a sua divulgação e nem sequer detêm meios para fazerem prevalecer o conjunto dos seus direitos previstos no RGPD (capítulo III).

4.3. UTILIZAÇÃO DOS DADOS DO CERTIFICADO PARA FINS NÃO LIGADOS A SITUAÇÕES DE SAÚDE PÚBLICA

Oskar Josef Gstrein,[102] ao examinar a proposta de texto para o regulamento do Certificado Digital manifesta a sua preocupação com situações em que os dados sensíveis possam ser utilizados para outras finalidades, diversas da que justificou a sua coleta. Traz exemplos de casos que revelaram quebra do compromisso em que a utilização dos dados de saúde seria feita apenas para situações de combate à doença.

Este ponto é da maior relevância. Oskar Josef Gstrein, num artigo que produziu com comentários e críticas ao Parecer Conjunto,[103] destaca: "*While the DPAs acknowledge that the Commission does not plan to establish a central database, questions have emerged about the oversight of data storage at the national level. In addition, even if the EUDCC is suspended at the EU level, it might be possible that nation states will continue to use their respective systems, which might also contain data originating from other Member States.*

---

[101] Não obstante o facto de se ter feito referência à alínea *g*) do inciso 2.º do artigo 9.º do RGPD, no Regulamento 2021/953, tratando-se de dados sensíveis de saúde tratados para os fins de interesse público no domínio da saúde pública, parece mais adequado convocar-se a aplicação da alínea *i*) e não há razão para se dispensar a exigência do sigilo. O RGPD refere-se a sigilo profissional, o que conduz à ideia de que aqueles que devem tratar dados de saúde, nas hipóteses da citada alínea *i*), devem ser profissionais de saúde e não terceiros sem essa qualificação.

[102] Oskar Josef Gstrein "The EU Digital COVID Certificate: A Preliminary Data Protection Impact Assessment" *in European Journal of Risk Regulation , Volume 12 , Special Issue 2: Symposium on COVID-19 Certificates and Special Issue on the Global Governance of Alcohol,* June 2021 , pp. 370 – 381 Disponível em https://doi.org/10.1017/err.2021.29 Cambridge University Press Consultado em 10.05.2022

[103] Cf. Oskar Josef Gstrein, *in The EU Digital COVID Certificate: A Preliminary Data Protection Impact Assessment,* Disponível em https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/eu-digital-covid-certificate-a-preliminary-data-protection-impact-assessment/F51BABA3959C62E1EE9EFDB26D21EBB9#fn16 10.12.2021

The question not only relates to how such data could be updated, revised or deleted. Even more concerning is a scenario where nation states adopt dedicated national laws to keep the systems originally intended for the EUDCC running and start to use them for other purposes such as national security. The updated draft addresses this issue in Article 9 paragraphs 3 and 3a but there is no comprehensive guarantee that one or more Member State(s) will not use the data from the EUDCC in other contexts based on national laws."

E, no mesmo artigo, Gstrein menciona casos que motivam a sua preocupação, a saber: i) a polícia de Singapura acedia aos dados dos aplicativos de rastreamento de contato apesar de promessas do governo local de que tal não seria admitido[104]; ii) a polícia alemã utilizou informações extraídas desses aplicativos de rastreamento, obrigatórios em *pubs* e restaurantes, para fins de investigação criminal; iii) as autoridades austríacas pretendiam inserir as informações obtidas com o certificado numa base abrangente de dados para vincular as informações com dados estatísticos relativos a histórico no trabalho, receitas, licenças de doença e educação, medida que teria sido bastante criticada.[105]

São situações que revelam o perigo, para autodeterminação digital, que envolve a coleta de dados pessoais de saúde para viabilização do Certificado Digital, e o risco para a efetividade do princípio da limitação da finalidade prevista no artigo 5.º, i, *b*) do RGPD.

4.4. FISCALIZAÇÃO – ACESSO A DADOS SENSÍVEIS POR PARTICULARES – DA SOCIEDADE DA INFORMAÇÃO PARA A SOCIEDADE DA VIGILÂNCIA

Segundo Shoshana Zuboff,[106] o capitalismo de vigilância inicia-se "*com a descoberta do excedente comportamental mais ou menos à-mão-de-semear no ambiente online, quando se percebeu que o «exaustor de dados» que entupia os servidores da Google podia ser combinado com suas potentes capacidades analíticas e com eles produzir previsões do comportamento dos utilizadores. Estes produtos preditivos seriam a base de um processo anormal de vendas lucrativas que criou novos mercados de comportamento futuro. A inteligência automática da Google foi melhorando à medida que o volume de dados aumentava, criando melhores produtos preditivos. Esta dinâmica determinou o imperativo de extração, o qual exprime a necessidade de economias de escala na acumulação de excedentes e que depende de sistemas automatizados que rastreiam, perseguem e induzem implacavelmente mais excedentes comportamentais. A Google impôs uma lógica da conquista,*

---

104 A esse respeito, veja-se a abordagem de Mia Sato *in MIT Technology Review*, Dispon+ivel em https://www.technologyreview.com/2021/01/05/1015734/singapore-contact-tracing-police-data-covid/. Consultado em 12.03.2022

105 *Cf.* Oskar Josef Gstrein *Ob cit*. pp 379/380

106 Shoshana Zuboff *-in A era do Capitalismo da Vigilância – A disputa por um Futuro Humano na Nova Fronteira do Poder*: Lisboa, Relógio D´Água Editores, 2019. p.374.

definindo a experiência humana como livre para recolher, disponível para renderizar na forma de dados e reivindicar como um ativo de vigilância. A empresa aprendeu a utilizar uma variedade de estratégias retóricas, políticas e tecnológicas para ofuscar esses processos e suas implicações."

A autora desenvolve o seu pensamento, descrevendo as fases mais avançadas de desenvolvimento desse processo e sustentando que os "*capitalistas de vigilância são empurrados do mundo virtual para o mundo real, com oportunidades de abastecimento ubíquo*", para que "*os produtos preditivos se aproximem da certeza e garantam resultados comportamentais*", para em seguida "*intervirem na situação corrente e moldarem de forma ativa o comportamento da própria fonte*".

É assustador este cenário que vai da vigilância à interferência no mundo real.

Mas os capitalistas não estão sozinhos neste processo apesar de serem inegavelmente o seu principal vetor. Assim, também os governos, cada vez mais, se assenhoreiam dos dados pessoais dos cidadãos, para controlo e interferência na sociedade.

E, com a pandemia da COVID-19, essa vigilância passou a ser largamente exercida, em nome dos interesses do Estado, pelos próprios cidadãos.

Como afirmou Zuboff: "*Seria incorreto assumir que o capitalismo da vigilância se consegue entender apenas pelo prisma da sua ação económica, ou que os desafios defrontados se restringem a discernir, conter ou transformar os seus mecanismos fundamentais. As consequências desta nova lógica de acumulação já ultrapassaram e continuarão a ultrapassar as práticas comerciais, influenciando a textura das nossas relações sociais, transformando o relacionamento connosco e com os outros. Estas transformações são o chão no qual o capitalismo de vigilância floresceu: uma espécie invasiva que cria a sua própria fonte de nutrição. Ao transformar-nos, alimenta a sua própria marcha*."[107]

A providência adotada pelos Estados-membros, de atribuir a particulares a fiscalização e verificação do Certificado nas situações enquadradas no largo espectro previsto na lei, como o acesso a eventos de natureza cultural, desportiva, corporativa ou familiar, representa mais um passo no sentido da vigilância das pessoas pelos seus pares.

Em certa medida, a situação revela como a sociedade tem optado por soluções jurídicas que restringem, cada vez mais, a liberdade individual, esvaziando o conteúdo dos direitos à privacidade. A sociedade da informação transforma-se progressivamente na sociedade da vigilância, com a participação disseminada de indivíduos nessa tarefa, estejam ou não munidos de poder estatal.

A situação, que decorreu das condutas de combate à pandemia, provocou a banalização da função de fiscalizar o atendimento a requisitos escolhidos pela

[107] Cf. Shoshana Zuboff *Ob. cit*. p. 384

lei para o exercício de direitos e liberdades. Patrões, empregados, empregados de lojas, restaurantes, salas de espetáculo, e toda uma coletividade de pessoas sem qualquer preparação ou responsabilidade legal passaram a exercer a função que deveria ser pública, de fiscalizar, impedir ou autorizar o exercício de direitos e de operar o tratamento de dados sensíveis, em auxílio ao Estado na tarefa de controlar o cidadão. E mais grave ainda é a tarefa de verificação da temperatura corporal (que também configura tratamento de dados de saúde) para fins de controlo de acesso ao local de trabalho, acesso a serviços ou instituições públicas, estabelecimentos educativos e espaços comerciais, culturais ou desportivos, meios de transporte, em estruturas residenciais, estabelecimentos de saúde, estabelecimentos prisionais ou centros educativos, como chegou a ser previsto no artigo 4.º do Decreto do Conselho de Ministros n.º 8/2020.

A reação das autoridades de proteção de dados diante dessa situação foi tíbia. A própria sociedade aceitou essas medidas ao pô-las em prática. É de facto uma tarefa difícil a de impedir, por qualquer meio, a adoção de estratégias que aparentam ser, num determinado momento, essenciais para o combate à pandemia e para o alívio das medidas rigorosas de *lock down*.

5. CONCLUSÃO

A crise causada pela pandemia, com a consequente necessidade de imposição de severas limitações sociais, sanitárias e pessoais à população mundial, em especial no seu direito de livre locomoção, acabou por gerar uma tendência nos governos para utilizar os dados especiais de saúde como instrumento de combate à propagação do vírus.

As empresas de tecnologia rapidamente desenvolveram aplicativos para rastreio dos infetados e dos seus contatos e estes passaram a ser uma ferramenta tentadora para se enfrentar a pandemia, controlando aqueles doentes ou suspeitos de estarem infetados, para concentrar sobre eles, e não sobre os demais, as restrições aos direitos e às liberdades de locomoção.

Outra forma de se atingir objetivo semelhante foi a criação de certificados sobre o estado de imunidade do cidadão, a partir de três vetores que indicavam o estado de vacinação, a recuperação recente da doença ou o teste de despistagem.

A discriminação entre portadores e não portadores do certificado, assim justificada pelo interesse público em se retomarem as atividades económicas, culturais e sociais, entretanto, acabou por pôr em causa a estrutura que fora criada para a defesa dos interesses dos titulares de dados pessoais, submetida a compreensível pressão para que a privacidade não fosse empecilho para a retoma das atividades económicas.

As entidades de defesa da proteção dos dados, alarmadas, advertiram sobre os riscos do que poderia vir a suceder. Primeiramente, tentou-se impor a utilização de aplicativos de geolocalização para controlo e rastreio dos infetados. Se a empreitada fosse bem-sucedida, o primeiro passo estaria dado para a verificação do temido cenário orwelliano de controlo da população. Mas a força do Direito foi intransponível e, pelo menos em Portugal, a medida não passou.

Mas nada foi capaz de impedir a adoção do certificado digital, inicialmente destinado a aliviar a população das restrições à livre circulação no âmbito da UE, e que teve o seu destino grandemente ampliado, para permitir a retoma das atividades daqueles que o tivessem.

Era expectável que tal ocorresse, diante do avanço da vacinação e do impacto que essa situação causou na redução dos casos e, especialmente, dos internamentos.

Mas isto não se deu sem que os direitos de privacidade dos titulares dos pessoais de saúde fossem atingidos. Admitir que se torne obrigatória ou quase-obrigatória a exposição de uma gama de informações de saúde a toda a hora e a quem quer que seja, para se poder entrar num restaurante ou num café, transformando esses dados em passaporte para atos rotineiros da vida, é esvaziar o conteúdo do direito à confidencialidade desses dados.

A convocação da população, impreparada e desprevenida, sem vínculo formal com o Estado ou mesmo consciência da importância e responsabilidades que cercam o tratamento de dados sensíveis, para a tarefa de fiscalizar o cumprimento da lei representou mais um passo no sentido da consolidação da sociedade da vigilância, em detrimento do direito à autodeterminação.

A pandemia deve passar. Já se foram os dias mais agudos e o porvir é alvissareiro. Mas as escolhas feitas hão de moldar as nossas vidas no futuro.

6. REFERÊNCIAS BIBLIOGRÁFICAS

Alves, Lurdes Dias – *Proteção de Dados Pessoais no Contexto Laboral*. Coimbra, Almedina, 2020. ISBN 978-972-40-8581-4.

Barata, Clara – "O que aprendemos sobre o covid-19 nos últimos dois anos" *in* Jornal Público (31 de dezembro de 2021). Publicação *online*, disponível em https://www.publico.pt/2021/12/31/ciencia/noticia/aprendemos-covid19-ultimos-dois-anos-1990319. (Consultado em 19.03.2022).

Canotilho, Gomes E Moreira, Vital – *Constituição da República Portuguesa Anotada. Vol. 1*, 4.ª ed. Coimbra, Coimbra Editora, 2007. ISBN: 9789725405413.

Carvalho, Jorge Morais – *Manual de Direito do Consumo*. 6ª ed. Coimbra, Almedina, 2019. ISBN 978-972-40-7833-5. P.56.

Carvalho, Orlando De – *Teoria Geral do Direito Civil*. 3ª ed. Coimbra, Coimbra Editora, 2012.

Cordeiro, A. Barreto Menezes – *Direito da proteção de dados: à luz do RGPD e da Lei n.º 58/2019.* Coimbra, Almedina, 2020. ISBN 978-972-40-8304-9.

Deodato, Sérgio – *A proteção dos dados pessoais de Saúde*. Lisboa, Universidade Católica Editora. ISBN 9789725405789, 2017.

Dias, Patrícia Cardoso – "Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública" *in Revista Julgar Online* de Janeiro de 2021-1. Disponível em http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/. (Consultado em 28.04. 2022).

Donald, Alice E Leach, Phillipe – "Human Rights – The Essential Frame of Reference in the Global Response to COVID-19" *in Verfassungsblog – On Matters Constitucional* 2020/5/12. Disponível em https://verfassungsblog.de/human-rights-the-essential-frame-of-reference-in-the-global-response-to-covid-19/ (Consultado em 10.04.2022)

European Center For Disease Prevention And Control – "Event Background COVID-19" Disponível em https://www.ecdc.europa.eu/en/novel-coronavirus/event-background-2019) (Consultado em 22. 04.2022)

Gstrein, Oskar Josef – Zwitter, Andrej E Kochenov, Dimitry – "*A Terrible Great Idea? COVID-19 'Vaccination Passports' in the Spotlight*" Disponível em https://www.compas.ox.ac.uk/2021/a-terrible-great-idea-covid-19-vaccination-passports-in-the-spotlight/ (Consultado em 09.05.2022)

Guimarães, Maria Raquel E Redinha, Maria Regina – "A Portuguese Approach to Privacy in COVID-19 Times: Through the Keyhole." *In Intersentia Online – Coronavirus and the Law in Europe"* 2021. Disponível em https://www.intersentiaonline.com/permalink/1fac1271118a21090498ddef1399707b. (Consultado em 12.05.2022)

Harari, Yuval Noah – "O mundo após o do coronavírus" *in Financial Times, edição de 20.03.2020*.]. Disponível em https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75. Consultado em 30.01.2022

Institute, Ada Lovelace – "What place should COVID-19 vaccine passports have in society?" *in Findings from a rapid expert deliberation – chaired by Professor Sir Jonathan Montgomery – Ada Lovelace Institute.* Disponível em https://www.adalovelaceinstitute.org/summary/covid-19-vaccine-passports/ (Consultado em 12.05. 2022).

Konder, Carlos Nelson – "O tratamento de dados sensíveis à luz da Lei 13.709/2018" *in – Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo, Thomson Reuters Brasil, 2019.

Miranda, Jorge – *A Constituição e a dignidade da pessoa humana*. Lisboa, Didaskalia, 1999 e *Curso de Direito Constitucional*. Lisboa, Universidade Católica Editora, 2016.

Oliveira, Fernando António Rodrigues Da Silva Coutinho – "Breves considerações a respeito do princípio da dignidade da pessoa humana" de 01.07.2013. Disponível em https://sigarra.up.pt/fdup/pt/pub_geral.pub_view?pi_pub_base_id=24817. (Consultado em 10.06. 2022)

Parlamento Europeu – "Proteção dos dados pessoais" Disponível em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf (Consultado em 28.01. 2022).

Pereira, Caio Mário Da Silva – *Instituições de Direito Civil*. 19ª ed. Rio de Janeiro, Forense, 2002.

Pinto, Paulo Mota – *Direitos de Personalidade e Direitos Fundamentais: estudos*. Coimbra, Gestlegal, 2018.

Saramago, José – *Ensaio sobre a Cegueira*. Lisboa, Livraria Lello e Porto Editora, 2021.

Sousa Ribeiro, J. – "A tutela de bens da personalidade na Constituição e na jurisprudência constitucional portuguesas". *In Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho*. Vol. III – *Direitos e Interconstitucionalidade: entre Dignidade e Cosmopolitismo*, Coimbra, Coimbra Editora. (ISBN 9789723220537) 2013.

Szaniawski, Elimar – *Direitos de personalidade e sua tutela*. São Paulo, Editora Revista dos Tribunais, 1993.

Tiffany C. LI – "Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis", *in Chicago Law Journal 767 (2021)*, Loyola University. Disponível em https://scholars.unh.edu/cgi/viewcontent.cgi?article=1459&context=law_facpub. [Consultado em 18.06.2022].

Vélis, Carissa – *in Privacidade é Poder, por que razão e como devemos recuperar o controle dos nossos dados, Temas e Debates*. Lisboa, Bertrand Editora. 2022. ISBN 978-989-644-688-8.

Warren, Samuel Dennis E Brandeis, Louis – "O Direito à Privacidade" *in Harvard Law Review*, *Vol. IV, 15 de dezembro de 1890*. Disponível em https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. (28.02.2022).

World Health Organization – "Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing" *in Interim guidance*, de 28.05. 2020: https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1 (acedido em junho 2022)

Zuboff, Shoshana – *in A era do Capitalismo da Vigilância – A disputa por um Futuro Humano na Nova Fronteira do Poder*. Lisboa, Relógio D´Água Editores, ISBN 978-989-783-090-7, (2019).

REFERÊNCIAS BIBLIOGRÁFICAS DO DOMÍNIO DA JURISPRUDÊNCIA

Tribunal de Justiça da União Europeia

Acórdão de 09.03.1978 – processo C-106/77 – SIMMENTHAL – (disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:61977CJ0106&from=DA)

Acórdão de 29.01.08, processo C- 275/06 Productores de Música de España (Promusicae)/Telefónica de España SAU, ECLI:EU:C:2008:54, (disponível em https://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06)

Acórdão de 8 de abril de 2014, – processos apensos C-293/12 e C-594/12, (disponível em https://curia.europa.eu/juris/liste.jsf?language=pt&num=C-293/12).

Acórdão proferido no julgamento dos processos apensos C-92/09 e C 93/09 (itens 47 e 48). (disponível em https://curia.europa.eu/juris/liste.jsf?num=C-92/09&language=en)

Acórdão proferido no julgamento dos processos c-112/00 – SCHMIDBERGER – (disponível em https://curia.europa.eu/juris/liste.jsf?num=C-112/00)

Tribunal Constitucional

Acórdão no Processo n.º 828/2019, acórdão n.º 268/2022, Plenário, Relator Conselheiro Afonso Patrão, julgado em 04.2022, (disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html)

Tribunal Europeu dos Direitos Humanos

Acórdão Application n.º 27798/95 – (caso AMANN v. SWITZERLAND), disponível em https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22Amann%20v.%20witzerland%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58497%22]}

TAX & DIGITAL ECONOMY: A TRIBUTAÇÃO DO MERCADO DE DADOS PESSOAIS

Inês Cardoso Brandão

inescardosobrandao@gmail.com

Resumo: A evolução tecnológica trouxe consigo o desenvolvimento de novas tecnologias, novas oportunidades de mercado e, com isso, novos modelos de negócios.

Com a inaptidão dos sistemas fiscais para a adaptação à rápida evolução da sociedade, criaram-se lacunas na Lei e, consequentemente, existência de rendimentos gerados e não tributados.

Para colmatar tais insuficiências, alguns países foram apresentando algumas propostas para a tributação das multinacionais digitais. No entanto, na sua maioria são de aplicação temporária com vigência até ao momento em que haja um acordo internacional ao nível da Organização para a Cooperação e Desenvolvimento Económico (OCDE). A OCDE, apesar de ter vindo a desenvolver interessantes trabalhos na área, através do Pillar One e o Pillar Two, ainda tem um longo caminho pela frente. E, essencialmente, algumas das dificuldades que enfrenta são: o colete de forças entre os vários países, a não capacitação das autoridades tributárias com ferramentas eficazes para conseguir captar os rendimentos das multinacionais e, ainda, a grande complexidade dos modelos de negócios digitais.

Porém, todas essas propostas são essencialmente sobre o rendimento das empresas por, maioritariamente, providenciarem serviços ou produtos online aos usuários de certa jurisdição.

Por outro lado, uma possível tributação sobre os dados pessoais e os gerados pelos indivíduos torna a situação difícil, visto que os dados não têm valor intrínseco e este é um dos requisitos da aplicação de um imposto: ser sobre a demonstração de riqueza (rendimento, consumo ou propriedade). No entanto, o exercício é feito e chega-se à conclusão que é, no mínimo, plausível discutir-se a aplicação de uma contribuição especial (se compararmos os dados pessoais com os recursos naturais) ou de um *royalty* (se a comparação for feita com os direitos de autor).

Apesar de não se chegar a nenhuma solução, conclui-se que o tema da tributação do mercado de dados é muito complexo, muito atual e, que, por isso, há que ter muita cautela ao tratar-se do assunto, principalmente, para que nenhuma suposta tributação venha causar uma repercussão fiscal no indivíduo, nem disrupções no mercado.

Palavras-chave: OCDE; Pillar One; Pillar Two; Digital Service Tax; Tributação de dados; Dados pessoais; Recursos naturais; Direitos de autor.

Abstract: Technological evolution has brought with it the development of new technologies, new market opportunities and, with that, new business models.

With the inability of the tax systems to adapt themselves quickly to the evolution of society, gaps remain in the Law and, consequently, the existence of generated and untaxed income.

To address such initiatives, some countries have presented proposals to tax the income of digital companies. However, most are just effective, until the moment there is an international agreement at the OECD level. The OECD, despite having been developing interesting works in the area, through Pillar One and Pillar Two, still has a long way to run. The major difficulties are, essentially, the diplomatic and power fights between the countries, the non-preparation of the tax authorities with capable tools to follow the performance of companies and, also, to be able to understand the great complexity of the digital business models.

However, all these solutions are mostly about the revenue of the digital companies coming from their online activity in certain jurisdictions.

On the other hand, a possible tax on personal data and data generated by the users becomes difficult to apply since the personal data have no intrinsic value, and this is a requirement for the application of a tax (needs to be over the income, consumption or property). However, the exercise concludes that it is plausible to apply a special contribution (if comparing the personal data to natural resources) or a royalty (if comparing to copyrights).

Despite the present work does not reach any solution, we conclude that the taxation of the data market in general is complex, actual, and, therefore, a lot of attention must be given to the treatment of the subject, mainly to avoid a supposed income to cause a fiscal repercussion on the individual or disturbances in the market.

Keywords: OCDE; Pillar One; Pillar Two; Digital Service Tax; Taxation of data; Personal data; Natural resources; Copyright.

1. INTRODUÇÃO

Nas últimas décadas a sociedade tem evoluído, paulatinamente, e veio com isso introduzir mudanças e colocar novas exigências.

Uma das principais reviravoltas que a sociedade observou, e que ninguém consegue negar ao fazer uma comparação com épocas passadas, foi a evolução tecnológica. Atualmente, somos inundados diariamente com tecnologia. E, se é verdade que os aparelhos eletrónicos nos rodeiam, também é verdade que o indivíduo se encontra no cerne de todo esse ambiente tecnológico.

As novas tecnologias trouxeram facilidades para o indivíduo e fizeram deste tanto o utilizador principal como o potenciador das mesmas.

Vejamos, os indivíduos ao utilizarem os aparelhos eletrónicos e os sítios na Internet, consciente ou inconscientemente, estão a fornecer os seus dados pessoais e os gerados por si, os quais vão ser recolhidos pelas empresas que estão por detrás do funcionamento do aparelho eletrónico ou da plataforma digital. Estas, posteriormente, vão analisá-los de forma a prever tendências ou as preferências dos usuários, ou então, apenas comercializar diretamente esses dados através da sua venda direta ou da venda dos estudos feitos com base nos mesmos. Portanto, é fácil o entendimento que na economia digital, mais concretamente no que diz respeito aos novos modelos de negócios digitais, o utilizador é tanto o recetor como o dador, criando-se assim um próprio mercado – o mercado dos dados. Invertendo a perspetiva, se os indivíduos deixassem de interagissem com as tecnologias, a economia digital teria um fim imediato.

Deste modo, percebeu-se que os utilizadores têm mais valor na economia digital do que anteriormente se pensava.

Com isto em mente, as questões sobre se as multinacionais digitais deveriam contribuir para a economia dos Estados começaram a colocar-se, pelo facto de estas: (1) serem operadores económicos, (2) por terem rendimento que não é capturado (3) e por utilizarem os utilizadores como base para o seu rendimento.

Mas, para serem tributados tais sujeitos, ter-se-á de decidir o que se quer tributar em primeiro lugar: ou se quer tributar os dados *per* se, os rendimentos gerados por aqueles, ou ambos.

Ora bem, é neste contexto, da tributação do mercado de dados, que o presente trabalho se irá focar. Isto inclui não só a tributação dos dados como objeto direto da tributação, como também a tributação direta dos rendimentos de negócios que fazem o uso dos dados dos usuários. A diferença está no objeto: enquanto na primeira opção o objeto da tributação são os próprios dados, na segunda o alvo principal da tributação são os rendimentos.

Para o estudo do mercado de dados a dissertação pretende analisar as várias vias possíveis de tributar desse mercado. Para esse âmbito, será analisada a proposta da OCDE e as soluções encontradas pelos países para a tributação dos rendimentos das multinacionais digitais. Como, de igual modo, serão apresentadas duas visões possíveis para a tributação dos dados *per se*. No entanto, antes de se passar para tal estudo, será abordada a matéria teórica sobre o nexo e sobre o escopo para a disciplina de Direito Fiscal. Isto, porque o objetivo primordial da presente tese prende-se com a demonstração, não só das razões e das várias possibilidades de tributação do mercado de dados pessoais, como também saber qual é o nexo e o escopo das possíveis propostas.

Este trabalho divide-se em três grandes capítulos.

No primeiro é feita uma breve introdução da matéria fiscal, explicando teoricamente dois dos elementos básicos da tributação – o nexo e o escopo.

O segundo capítulo trata da tributação dos rendimentos provenientes da utilização dos dados dos utilizadores, baseando-nos para o efeito na análise da proposta da OCDE, intitulada, Pillar One, e nas soluções que os diferentes países foram encontrando para tributar as multinacionais digitais.

No terceiro, é introduzido o estudo de duas visões vanguardistas de uma possível tributação dos dados pessoais por si mesmos.

Por último, o trabalho termina com um resumo do estudo desenvolvido ao longo do trabalho e com algumas considerações.

Por fim, alerta-se o leitor de que o objetivo desta dissertação é explanar as várias hipóteses que têm vindo a ser debatidas para a tributação do mercado de dados pessoais. Também se deve referir que, enquanto, no segundo capítulo são analisadas as várias propostas ou soluções já em vigor sobre a tributação do rendimento das multinacionais digitais, no terceiro capítulo são introduzidas para discussão duas visões possíveis de como tributar os dados pessoais, ou pelo menos a discussão da razão por detrás de tal tributação.

Dentro do tema, por questões de simplicidade e espaço, o foco, apenas, será direcionado ao nexo e ao escopo. Não importando para o trabalho as outras vertentes, como por exemplo, a discussão do novo conceito de estabelecimento estável (EE), ou a discussão de como os direitos tributários devem ser alocados se já não é possível o recurso à presença física do operador económico, ou se haverá dupla tributação e como esta deve ser eliminada, entre outros.

2. CONTEXTO

Foi com a revolução industrial, datada no período entre o final do séc.XVIII e início do séc.XIX, em Inglaterra, que marcou o início do desenvolvimento acentuado das tecnologias. Um pouco mais tarde, no início do final do séc. XIX e durante o séc.XX, começou a dar-se os primeiros passos na criação de equipamentos eletrónicos que tivessem a capacidade de comunicar e trocar informação entre si.

O primeiro instrumento eletrónico de informação e comunicação a ser criado foi o telefone, mesmo antes da viragem do século, em 1876, quando foi registada a patente por Graham Bell, contudo, apenas podia ser utilizado em curtas distâncias. Anos depois, Edison, em 1877, desenvolveu a ideia do telefone e inventou um aparelho que utilizava um microfone de carvão e que podia ser utilizado já em longas distâncias. Mais tarde, a marcar o início do séc.XX, mais concretamente em 1901, surgiu a primeira transmissão de um sinal rádio, que atravessou o Oceano Atlântico, conseguida por Guglielmo Marconi. Com as grandes guerras, principalmente durante a II Guerra Mundial, foi desenvolvido o radar pelas mãos de Robert Watson-Watt, e por volta do final dos anos 40 foi inventada a televisão por Philo Farnsworth e desenvolvida por Vladimir Zworykin.

O primeiro computador pessoal de sucesso foi o Apple II criado por Steve Jobs e Steve Wozniak. Após este momento começou a inovação de *softwares* que fossem capazes de ler e tratar informações de forma rápida. Nos últimos anos houve uma explosão dos computadores portáteis e, de seguida, mais recentemente, dos *Tablets*. Atente-se ainda que os computadores vieram também permitir a criação de outros novos instrumentos, tais como os *GPSs*.

Estava então tudo reunido para que aparecesse uma das grandes marcas da viragem do séc.XX para o séc.XXI - a Internet. Este instrumento veio revolucionar o modo como as pessoas comunicam e como a informação circula a nível mundial. A Internet resume-se a uma rede global que liga os computadores e permite que estes troquem informações entre si, via satélite, por cabos de fibra ótica, ou linhas telefónicas. Esta nova invenção veio potenciar a globalização e transformar a economia e a sociedade num todo.

Aliás, como a sociedade está em constante movimento, as tecnologias também se foram desenvolvendo ao ritmo e às necessidades da sociedade, às vezes na sua dianteira, mas maioritariamente em resposta às carências levantadas por aquela.

Porém, hoje em dia já não se fala mais na Internet como a invenção do século, atribuindo-se esse prémio agora à Inteligência Artificial.

A Inteligência Artificial não é mais do que um computador que tem como objetivo imitar o cérebro humano. Vejamos, a inteligência artificial não é nada mais do que um computador munido com uma base de dados e al-

goritmos. O que acontece, sumariamente, é o seguinte: o aparelho recebe a informação externa, que serão os dados (por meio de voz, imagem, ou por outros meios que podem ser apreendidos pelos sentidos), sendo que os algoritmos inseridos no computador analisam esses dados recolhidos e recorrem à base de dados de que tem posse para daí retirarem um conhecimento e, posteriormente, exteriorizá-lo através de uma resposta (que seja passível de ser apreendida pelos sentidos do recetor).

Este é um dos muitos usos dos dados.

Os dados são hoje em dia o motor da tecnologia, sendo de difícil exercício encontrar uma que não funcione à base de dados. No entanto, a arrecadação de dados não é novidade, assim, nas décadas passadas as máquinas já eram capazes de receber informação e analisá-la. A coleção e a monetização dos dados dos indivíduos não são necessariamente novas. Se recuarmos até aos finais dos anos 1800, já era prática a manutenção de listas de consumidores para desenhar programas de negócios[1]. Porém, foi devido à evolução tecnológica, que esta possibilitou a recolha e o processamento de grandes quantidades de dados, que colocou essas atividades no cerne dos modelos de negócios digitais de muitas das companhias digitais e que estão presentes na economia digital.

Assim, a novidade está na quantidade gigantesca que as novas tecnologias conseguem arrecadar e analisar. Como se referiu, os dados não são nada mais do que informação pura, mas a importância está no tipo de informação que contêm. Ora, a maior parte do debate acerca dos dados diz respeito aos dados pessoais e a outros, que não sendo considerados pessoais, são dados gerados pelos indivíduos[2] – os chamados *Big Data*.

Este tipo de dados é importante não só para o funcionamento das tecnologias em geral como para a digitalização da própria economia.

Já várias vezes referido, os dados pessoais e os dados gerados pelos usuários (que vamos passar, por questões de simplicidade, a referir-nos a apenas aos dados pessoais incluindo na expressão também os dados gerados pelos usuários)[3] são considerados o "novo petróleo".

---

[1] Aqib Aslam, Alpa Shah, *Tec(h)tonic Shifts: Taxing the Digital Economy*, IMF Working Paper. P.8. (Disponível em: <https://www.imf.org/en/Publications/WP/Issues/2020/05/29/Tec-h-tonic-Shifts-Taxing-the-Digital-Economy-49363>)

[2] Os dados pessoais são dados que são identificativos do indivíduo que os doou, como por ex., o nome, idade, morada, número de identificação. Já os dados gerados pelo indivíduo não são dados que possam identificar diretamente uma pessoa, mas são por ela criados quando faz uso das interfaces digitais, por ex., quando abre um *link* no sítio da Internet, dá um gosto, faz um comentário, faz uma compra.

[3] Há ainda outra distinção que é feita quanto à forma de provisionamento dos dados dos usuários: passivo e ativo. O primeiro é caracterizado pelo fornecimento de dados de forma inconsciente enquanto se faz uso dos serviços digitais, já o segundo será quando os usuários contribuem nas redes de media ou quando a sua participação é diretamente solicitada (por ex., em forma de questionário ou reclamação). Quanto à coleção passiva

Isto porque, passa-se a explicar: a maioria da economia digital, onde operam as grandes multinacionais digitais (como a Facebook, a Amazon, a Google, entre outros), funciona em volta dos dados pessoais e por causa deles. A maioria destas empresas presentes tem como seu principal negócio a comercialização dos dados, ou pelo menos a comercialização do seu estudo, ou recolhe-os e trata-os para utilização deles no seu próprio negócio.

Daí que é cada vez mais comum se ouvir dizer que os dados pessoais são potenciadores de valor para as empresas, porque através da sua recolha e/ou tratamento conseguem gerar rendimento no futuro, quer pela comercialização dos dados, quer pelo melhoramento do serviço ou produto prestado, baseado neles.

A recolha dos dados dos usuários no mundo digital acontece de forma distinta do presencial. A interação dos indivíduos com os serviços digitais dá-se de variadas formas. Quando há uma compra online, o consumidor revela informação sobre as suas preferências, as quais são registadas pela empresa para no futuro serem utilizadas e monetizadas; portanto, no momento da compra o consumidor não só efetua um pagamento em troca de um serviço ou bem, como fornece dados quando utiliza a plataforma digital para fazer a tal compra, independentemente, se é uma plataforma de intermediação entre o comprador e o vendedor. Outra forma de interação é quando o usuário utiliza um motor de busca "gratuito" na Internet ou aplicação móvel, neste caso, é considerado que em troca do acesso ao conteúdo online, o usuário dá em troca informação sobre si e sobre os seus interesses. Ainda, na interação entre indivíduos online, através das famosas plataformas de media social, quando os usuários partilham e geram conteúdo digital (como vídeos, experiências, fotos, entre outros) eles estão automaticamente a revelar informações sobre eles mesmos que são capturadas pelas plataformas. E, ainda, quando um indivíduo faz uso de um aparelho que está conectado com a Internet ("*Internet of Things*"), está a enviar dados através dos sensores que estão embutidos no objeto, que tanto os recebe como os envia para o operador do sistema (como por ex., os termostatos, os aspiradores, carros e escova de dentes eletrónicas)[4]. Algumas empresas seguem

de dados há quem argumente que a "produção" dos dados em bruto deve ser atribuída à empresa e não ao usuário visto que o seu papel é desde logo limitado pelo seu prévio consentimento (Becker e English, 2019) e, por isso, a sua mera aquiescência para se ser observado não deve ser considerada como cocriação de valor, sendo assim, estes argumentam ainda que, só quando os dados dos usuários são ativamente solicitados ou providenciados é que se deve considerar que há criação de valor pelos próprios usuários. No entanto, na visão de Aqib Aslam e Alpa Shah, esta discussão é irrelevante pelo facto de que em ambas as situações, seja o provisionamento ativo ou passivo dos dados, os dados têm valor e podem ser monetizados. *Supra* nota 1, p.10.

[4] *Supra* nota 1, p.8-9

ainda a atividade do usuário mesmo quando este não está a fazer uso da plataforma, através do uso dos *"tracking cookies"*[5] e da recolha de dados[6].

A combinação da necessidade dos Estados em fazer frente a novas crises económicas com o enorme volume de rendimentos das grandes multinacionais (refere-se aqui essencialmente às digitais) resulta em que os Estados, desesperadamente, tentarão encontrar novas formas de tributação desse rendimento que não está a ser capturado para as contas nacionais, maioritariamente, por existirem lacunas na Lei.

As motivações que levam à tributação da economia digital podem ser várias, desde a maior justiça fiscal entre as várias empresas, como para uma maior igualdade entre os Estados[7]. No entanto, a principal motivação política é, normalmente, a de captura de mais receita para as contas estatais. Outra razão, muito pouco defendida, que pode também ser usada para a justificação da tributação das digitais é a questão ambiental, devido ao significativo impacto ambiental da coleção, armazenamento e tratamento dos dados[8].

Coisa diferente da motivação, normalmente politizada, é o estabelecimento de um vínculo entre uma dada jurisdição e o seu direito a tributar: o *nexus*. Ou seja, é a legitimação de um certo Estado sentir-se no direito de tributar determinada realidade. Não adianta um Estado querer tributar determinado facto por este ser rentável ou por expressar riqueza que legitima o Estado a impor uma tributação sobre tal.

2.1. NEXO

O poder da tributação, i.e., o poder de impor e exigir impostos pertence quase exclusivamente aos Estados. Aos Estados é-lhes reconhecido a ca-

---

5 *Supra* nota 1, p.10

6 Pense-se, por exemplo, no caso da Siri, um assistente virtual presente nos aparelhos da Apple utilizado para responder a perguntas ou a pedidos do usuário. Para a sua ativação basta o usuário chamar pelo nome "Siri" para ativar o serviço. Mas, para que o serviço reconheça que a palavra-chave ("Siri") foi pronunciada tem de estar então a escutar ininterruptamente o usuário para saber quando este a profere.

7 Pense-se no caso do Facebook, este grupo adquire os dados dos cidadãos dos vários pontos do globo, atuando digitalmente em várias jurisdições, para depois com esse poder vender serviços (como a publicidade online) baseados nos tais dados, mas como a sede do grupo está sediada nos Estados Unidos da América (EUA), então será apenas aí que será tributado. Ou seja, o valor é adquirido num determinado país, mas afinal quem beneficiará será apenas o país da sede, e não aquele onde houve a criação de valor. Assim, a polémica instala-se e os Estados sentem-se no direito de também imporem uma tributação. Situação que em tempos criou um braço de ferro entre os EUA, onde se encontram sediadas as maiores tecnológicas, e a Europa, onde aquelas têm uma grande presença junto dos usuários europeus.

8 Emmanuelle Deglaire, *Taxation of data: the next step?* (Disponível em: <http://link.library.ibfd.org/portal/Taxation-of-data--the-next-step/yWWexBFP7f0/>). P.3.

pacidade de impor e submeter aos seus comandos os seus cidadãos, através da ordem legal (por via da legislação) – *"force qualified by the law"*[9].

O Estado é instituído com esse poder pelos documentos constitucionais da nação (no caso português, a Constituição da República Portuguesa [CRP]), é aí que encontra a sua razão, mas também as suas limitações. É no documento constitucional que estão os valores pelos quais o Estado se deve reger: valores e princípios que são tidos como fundamentais para os cidadãos.

Reconhecida a soberania[10], o Estado passa a ser considerado um Estado soberano. Isto significa que adquire o poder supremo sobre um dado território e tal é reconhecido pelos outros Estados. A soberania tem então duas vertentes: o Estado soberano tem poder dentro das suas fronteiras e só a ele pertence a legitimação para exercer tal poder (soberania positiva), tal como essa legitimação só se circunscreve ao seu território, não podendo o Estado intrometer-se nos assuntos dos outros Estados (soberania negativa). Como constatado por Brownlie, a soberania e a igualdade dos Estados representam a doutrina constitucional básica do direito das nações, que governa a comunidade composta principalmente de Estados dotados de personalidade jurídica uniforme[11].

Sendo reconhecida a soberania de um Estado, este tem poderes e deveres dentro das suas fronteiras, a jurisdição[12]. Um desses poderes é o poder de exigir o pagamento de impostos.

A própria CRP refere-se ao sistema fiscal como o meio para a "satisfação das necessidades financeiras do Estado e outras entidades públicas e uma repartição justa dos rendimentos e da riqueza". Tal missão caberá à Assembleia da República ou ao Governo (art.165º, nº1, al.i) e 198º, nº1, al.b) CRP), que têm o poder legislativo para determinar "a incidência, a taxa, os benefícios fiscais e as garantias dos contribuintes" na criação de cada tributo (art.103º e 104º CRP).

Este poder de tributação dos Estados é de tal forma importante, que a partir dos inícios do séc.XX, quase todos os Estados modernos poderiam ser apelidados de *"tax state".* Esta conotação vem do facto do Estado arrecadar mais de metade da sua receita via impostos, para que posteriormente

---

9 Stjepan GadžO*, Chapter 2: Legal Fundamentals of Income Tax Jurisdiction in Nexus Requirements for Taxation of Non-Residents' Business Income – A Normative Evaluation in the Context of the Global Economy*. (Disponível em: <https://www.ibfd.org/shop/book/nexus-requirements-taxation-non-residents-business-income-normative-evaluation-context>).

10 Os princípios da soberania de um Estado foram afirmados na *Paz de Westphalia*, e são eles: o princípio da delimitação territorial do poder estatal que, em determinado território, é considerado último e independente do poder religioso; e o princípio da não ingerência nos assuntos internos do Estado. *Supra* nota 9.

11 *Supra* nota 9.

12 Jurisdição é o poder de o Estado determinar o que é lei e como ela se vai executar. É, portanto, o direito do Estado de regular dentro das suas fronteiras (que se consubstancia nos seus três poderes do Estado: legislativo, judicial e administrativo). *Supra* nota 9.

o mesmo grupo de contribuintes usufrua de serviços públicos financiados[13]. Pois, claro está que, *"taxes are what we pay for civilized society"*[14].

Não obstante, os Estados, como se disse, têm os seus poderes soberanos limitados, seja pelos documentos constitucionais, seja pela inserção na Comunidade Internacional. E, os mesmos limites aplicam-se de igual forma ao poder de tributar. O Estado não tem livre-arbítrio na criação e imposição de tributos, até porque está desde logo obrigado a respeitar o princípio da legalidade.

Uma das exigências para a criação de um tributo é a existência de um *nexus*.

O nexo é o estabelecimento de uma ligação direta entre o Estado, que aspira a exercer os seus poderes de tributação, com um conjunto particular de factos relevantes para a tributação. Assim que a conexão é estabelecida, o exercício dos poderes tributários por um Estado passa a ser vista como legítima, tanto para os cidadãos como para a Comunidade Internacional[15].

A forte ligação entre o contribuinte e o Estado por via de certo facto tributável (rendimento, consumo ou propriedade) é o requisito para a existência do nexo e, consequentemente, a legitimação para tributar.

Estabelecendo-se o *nexus*, então, o Estado ficará legitimado a criar um tributo (contribuição, taxa ou imposto), a alocar os direitos tributários, a determinar a base tributária e todas as outras características do imposto.

A fonte que estabelecia frequentemente o *nexus* entre um facto tributável e um Estado, através do princípio da territorialidade, era o conceito de Estabelecimento Estável (EE). Contudo, a economia digital é fortemente caracterizada por serviços que correm no âmbito digital e que, por isso, prescindem de uma presença física. A característica-chave dos serviços digitais é exatamente a não dependência de um local físico para operar, deixando cair por terra a importância que outrora o conceito de EE tinha para o Direito Fiscal.

Um dos grandes desafios que a economia digital coloca para o Direito Fiscal é exatamente não ter necessidade de uma presença física para uma determinada empresa poder operar numa determinada jurisdição, situação que é comumente utilizada para estabelecer a relação Estado-sujeito passivo.

Ora, esta nova realidade trouxe muitas dificuldades aos governos, principalmente no desenho de um *nexus* entre estes serviços digitais e a sua jurisdição para a alocação de direitos tributários.

As justificações pelas quais um Estado quererá tributar os dados pessoais podem ser variadas, ainda que a única exigência é o estabelecimento do nexo entre a situação que se quer tributar e o Estado, caso contrário este não estará legitimado para impor um tributo.

---

13 *Supra* nota 9.

14 Frase atribuída ao jurista americano Oliver Wendell Holmes, Jr. (1841-1935). *Supra* nota 9.

15 *Supra* nota 9.

2.2. ESCOPO

Estabelecido o *nexus*, cabe então determinar o âmbito da aplicação do tributo ou imposto, nomeadamente: saber quais as situações de facto que se vai querer tributar, e daí, consequentemente, que sujeitos vão ser submetidos ao cumprimento da obrigação tributária.

Qualquer tributo que se queira implementar tem de ter obrigatoriamente uma incidência. A incidência pode ser objetiva ou subjetiva, dependendo se se está a falar do objeto ou do sujeito.

Nos termos do art.18º, nº3 Lei Geral Tributária (LGT), "o sujeito será a pessoa singular ou coletiva, o património ou a organização de facto ou de direito que, nos termos da lei, estejam vinculados ao cumprimento da prestação tributária, seja como contribuinte direto, seja como substituto ou responsável".

Posto isto, o sujeito será sobre quem vai recair a obrigação tributária. Já o objeto (não o objeto da relação jurídica tributária), por seu turno, compreenderá o alvo material do tributo ou imposto, i.e., as atividades ou situações que se querem tributadas.

Com isto em mente, parece fácil a aplicação teórica destes requisitos na tributação do mercado de dados: o objeto seria então os dados pessoais e os sujeitos seriam os operadores económicos que recolhessem e tratassem aqueles. Mas, desengane-se: um dos grandes desafios é a determinação do valor dos dados.

Tal determinação é importante para a existência de qualquer tributo, pois este vai aplicar-se sobre um determinado valor. A contribuição incide sobre o custo do desgaste ou o valor do benefício, a taxa aplica-se sobre o valor do serviço administrativo prestado, e o imposto recai sobre o valor do rendimento, o valor do produto ou serviço comprado ou o valor da propriedade. Sabendo isto de antemão, e sabendo também que os dados não têm um valor, a aplicação de um tributo sobre esses fica difícil.

Os dados em si mesmos não têm qualquer valor intrínseco nem a sua determinação é simples. Muitos argumentam que os dados pessoais, quando coletados, já são presumivelmente valiosos e que, por isso, já é possível descobrir o seu valor; mas também não encontram um método eficaz que consiga, com a menor margem de erro possível, estimar o *quantum* desse valor é efetivamente se verificado. Outros defendem que os dados pessoais só adquirem valor quando a empresa que os analisa aplica o seu *know-how* e a sua tecnologia para retirar do estudo dos dados as conclusões que a vão ajudar posteriormente a tomar decisões quanto ao seu negócio. E, ainda, uma terceira visão é de que os dados apenas ganham valor quando há uma venda ou transmissão dos dados pessoais, pois é estipulado um preço entre as partes por essa transação; no entanto, este valor é subjetivo, pois dependerá da importância que as partes intervenientes atribuem àqueles dados

ou a bases de dados; pois, claro está, que o preço seria diferente se estivessem em causa outros operadores, não determinando assim efetivamente o seu valor intrínseco.

a) Determinação do valor dos dados

Ora, assim está colocada a primeira dificuldade para a tributação do mercado de dados, qual o seu valor? – qual é o valor dos dados pessoais?

O ponto de partida é de que o valor dos dados não poderá ser determinado levando apenas em conta o volume dos dados que são detidos ou transmitidos. Isto, porque o valor dos dados dependerá do contexto onde se inserem, de onde são recolhidos, para que fim vão ser utilizados e que informação contêm[16][17].

Fácil seria resolver o assunto dizendo que as bases de dados poderiam ser entendidas como ativos intangíveis de forma a entrarem na contabilidade das empresas. O que tornaria tudo mais simples e rápido, pois seria possível saber quanto as empresas detinham.

Contudo, a realidade demonstra algo diferente. No entendimento da *International Accounting Standard*, as bases de dados até podem ser apreendidas como ativos, mas se, e só se, for provável que a entidade irá futuramente obter benefícios económicos devido àquele ativo e se o custo deste for possível medir de forma fiável. Nestes termos, entrariam facilmente as compras das bases de dados, mas ficariam excluídas aquelas que são geradas dentro da mesma empresa ou grupo, que por acaso representam a maioria dos casos. Na mesma linha vai o *System of National Accounts* que entende que as bases de dados deveriam ser entendidas como ativos de propriedade intelectual no caso de essas bases deterem dados com uma vida útil por mais de um ano. Porém, também esta tem a sua praticabilidade comprometida quando nos apercebemos que com a rápida transação de informação de dados, torna-se difícil cumprir este requisito da sua manutenção por mais de um ano[18].

Neste contexto, com as dificuldades em estipular um método de valoração de dados, a OCDE decide analisar quatro possíveis fórmulas que se mostram potenciais vias na determinação do valor dos dados[19].

---

16 OCDE, Daniel Ker, Emanuele Mazzini, *Perspectives On The Value Of Data And Data Flows*. (Disponível em: <https://www.oecd-ilibrary.org/docserver/a2216bc1-en.pdf?expires=1646309134&id=id&accname=guest&checksum=7D020ED210C6B8C2F19E9A09E1A081FE>). P.8.

17 Na maioria das vezes, os dados ou bases de dados só adquirem um valor quando há uma compra e venda dos dados ou bases de dados, ou uma licença para o seu uso. Será no âmbito da negociação, estipulando-se um preço, que se determina o valor que aqueles dados têm. Este valor é subjetivo pois dependerá da importância que as partes intervenientes atribuem àqueles dados ou bases de dados; pois, claro está, que o preço seria diferente se estivessem em causa outros operadores económicos.

18 *Supra* nota 16, p.9 a 11.

19 Tal relatório analisa-se neste presente trabalho de forma superficial, pelo que para maior aprofundamento recomenda-se a leitura integral do relatório. *Supra* nota 16.

A primeira solução estudada pela OCDE no relatório é intitulada *"data storage"*[20].

Resumidamente, é uma fórmula que, com recurso a tabelas sobre o fornecimento-uso de dados (*supply-use*) e a bases de dados de estatísticas dos negócios, visa obter o valor dos dados pela despesa que as empresas têm em produtos de armazenamento de dados (*hardware, software* e serviços)[21]. Isto significa que, com recurso aos dados disponibilizados pelos vários países, conseguir-se-á, através do volume de despesa feita na compra e/ou utilização de produtos para armazenamento de dados e/ou em produtos de *software* de gestão de bases de dados, obter uma estimativa do valor desses.

A grande questão levantada por esta fórmula será a de saber que tipo de custos entrarão para a soma dos gastos e, consequentemente, a sua classificação. Neste ponto, não é dada pelo relatório nenhuma solução fiável, visto que nenhuma das duas formas estudadas cobre totalmente as classes de produtos envolvidas no armazenamento de dados e na gestão das bases de dados.

A segunda fórmula põe a tónica no rendimento gerado pelas empresas que criam um valor explícito através dos dados[22]. E, para tal, utiliza como recurso as fontes de estatísticas dos negócios.

Esta fórmula – *"Output of firms compiling and selling databases"* – foca-se apenas nas atividades económicas que produzem e vendem informação compilada em bases de dados[23].

Não diferente da primeira, esta fórmula apresenta também os seus desafios. Ora, a primeira problemática prende-se em saber que tipos de indústrias estão em causa e quais as empresas incluídas e que compilam e vendem bases de dados. Para saber quais serão as indústrias-alvo, poder-se-á recorrer, na ótica da OCDE, à própria classificação das indústrias e daí verificar aquelas que incorporam atividades ligadas à compilação e venda de bases de dados. No entanto, a classificação das indústrias põe o foco na atividade principal das empresas, pelo que aquelas empresas que têm como atividade secundária a compilação e venda de bases de dados ficarão de fora. O recurso ao mapeamento dos produtos por indústria poderia ser outra forma de lá chegar. Apesar disso, ambos os métodos de recurso enumerados sofrem de falta de informação e de pouca conformidade entre os países na descrição das indústrias.

---

20 *Supra* nota 16, p.9 ss.

21 Quanto às bases de dados, há sempre duas componentes presentes: *data storage* e *database management software*. A primeira integra o armazenamento físico de dados (*storage hardware* e *storage media*) e/ou o serviço de armazenamento de dados (ex.: armazenamento na *cloud*, i.e., "nuvem"); já o segundo diz respeito ao *software* de gestão de bases de dados utilizado pela entidade. *Supra* nota 16, p.9 a 11.

22 *Supra* nota 16, p.20.

23 Atente-se, no entanto, que esta métrica de valoração dos dados refere-se apenas às atividades onde há uma compra e venda direta de bases de dados (que pode ter várias formas, tais como, a venda por isso só, a subscrição para acesso, licença). *Supra* nota 16, p.20.

A terceira fórmula com o título *"data and firm values"* utiliza como instrumento as "*data-driven firms*", que são aquelas que o seu *core business* inclui na recolha, no armazenamento e/ou na análise de grandes quantidades de dados[24].

Fala-se aqui, e diferentemente da segunda fórmula, das bases de dados que são criadas e analisadas (e que incluem os dados dos consumidores), não para serem vendidas, mas para serem utilizadas dentro da própria empresa ou do grupo. E, apesar de não serem vendidas, o desenvolvimento de bases de dados gera igualmente valor pois contribuí para o preço alcançado nas aquisições das empresas. Desta forma, não se pode olhar para o valor duma empresa somente pelo seu trabalho com dados, pois na maioria dos casos, o armazenamento e tratamento dos dados por uma empresa, apesar de ajudar a melhorar o produto/serviço, não é a sua principal ou única atividade, ou pelo menos não depende inteiramente dos dados que possui[25]. Mas, claro está, há também casos que se encaixam perfeitamente nesta terceira fórmula, ou seja, empresas que devem o seu valor de mercado inteiramente às suas bases de dados e à habilidade em as analisar e monitorizar[26].

O fatal problema desta fórmula é a não existência rigorosa de um registo das empresas que se caracterizam por o serem e que são maioritariamente *data-driven*, i.e., onde o seu negócio passa inteiramente pelo armazenamento e utilização de dados, e que a isso devem o seu valor de mercado.

Por último, a quarta fórmula com o nome *"Perspectives on the value of cross-border data flows"*[27], prende-se, como o próprio nome indica, com a transmissão internacional de dados.

Haverá movimentos internacionais de dados, quando, de um aparelho de armazenamento localizado num dado país, há um movimento de dados para outro aparelho que se encontra localizado noutro país.

Para a valoração das transferências além-fronteiras de dados, esta fórmula considera o volume e o valor associados aos movimentos internacionais de dados. Porém, a grande dificuldade está em saber se o volume de dados que navega na Internet está associado ao comércio ou não, e saber qual a ligação direta desse movimento para a criação de valor para a empresa que o faz. Outra dificuldade é a de distinguir os fluxos que cruzam fronteiras daqueles que se movimentam dentro da mesma jurisdição. Para maior complicação, surgiu uma nova realidade: os chamados *"Internet Service Providers' networks*" (*ISPs networks*) que fazem com que, na maioria das

---

24 *Supra* nota 16, p.50.

25 Veja-se os exemplos da Amazon e Uber: são duas empresas que têm modelos de negócios baseados em dados, os chamados *"data-driven business models"*, mas têm também o complemento físico de entrega de bens e serviços, ou seja, o seu negócio baseia-se em grande parte nos dados, mas não totalmente. *Supra* nota 16, p.51

26 Fala-se aqui dos casos da Google, Facebook, etc. *Supra* nota 16, p.8.

27 *Supra* nota 16, p.56 ss.

vezes, nem haja qualquer movimento internacional de dados, pois os estes são transmitidos dentro de *ISPs networks*[28].

Assim, tal como nas anteriores, a questão da insuficiência de informação é fulcral para o desenvolvimento e eficácia da fórmula.

Em suma, a primeira fórmula tenta estipular o valor dos dados através dos gastos que as empresas fazem na compra e/ou utilização de produtos para armazenamento de dados ou gestão das bases de dados; a segunda fórmula tenta determinar o valor do rendimento gerado pelas empresas quando vendem dados e bases de dados; já a terceira fórmula utiliza as empresas que têm no cerne do seu modelo de negócio o armazenamento e o tratamento de dados; por último, mas não menos importante, a quarta fórmula recorre ao valor económico associado ao fluxo internacional de dados.

Conclui-se quanto a este tema que a tentativa da OCDE em surgir com uma solução eficaz para determinar o valor dos dados na economia digital fracassou inteiramente, devido à dificuldade e complexidade do tema; mas, também em grande parte, devido à falta de informação detalhada e necessária para cada uma das quatro fórmulas apresentadas.

Apesar de não haver uma conclusão de qual das fórmulas será a mais viável, consegue-se já criar quatro caminhos possíveis para futuro desenvolvimento sobre o tema.

3. TRIBUTAÇÃO DA ECONOMIA DIGITAL

Tendo-se estudado anteriormente a matéria do nexo e da incidência fiscal e a sua importância para a tributação, estamos agora aptos para começar a análise das várias propostas apresentadas para a tributação do mercado de dados, começando agora por aquela que foi apresentada pela OCDE.

3.1. PROPOSTA DA OCDE

Como visto anteriormente, um dos *players* mais importantes no motor da economia digital são os dados, essencialmente os dados dos usuários. E, dada a sua relevância, tanto a dependência dos dados, como a sua recolha e exploração, foram até mesmo tidos pela OCDE como sendo um fator de potencial relevância para o contexto fiscal e que comportam novos desafios

[28] Serve de exemplo a Netflix. Uma subscrição da Netflix em França poderia criar fluxos de comércio de dados audiovisuais entre os EUA e França, contudo, na realidade, esta situação não gerará nenhum fluxo internacional de dados, visto que a Netflix coloca servidores de conteúdo dentro dos países com o objetivo de otimizar a performance do serviço, minimizando a distância física pelo qual o conteúdo tem de viajar, e de evitar colocar muito peso nas infraestruturas da Internet. *Supra* nota 16, p.80 a 81.

para as atuais regras fiscais[29], ao lado de tantos outros desafios que a digitalização da economia criou para o Direito Fiscal[30].

Para dar, então, resposta à digitalização da economia, incluindo a questão da criação de valor através dos dados e da participação dos usuários, a OCDE reconhece a necessidade de uma resposta global no relatório de 2018[31].

Apesar disso, neste relatório a OCDE admite que o nível de uso dos dados dos consumidores, ou da sua participação, pode não estar diretamente relacionado com o nível de digitalização de um negócio. E, por isso, a OCDE claramente distancia-se de uma solução unicamente focada nos dados, sob pena de muitos dos negócios digitais ficarem de fora por essa mesma razão. Daí que na solução posteriormente em estudo, a OCDE apresenta uma via em que integra a questão da criação de valor através da colheita e utilização de dados, apenas como uma parte da resposta a dar aos negócios digitais, de forma a conseguir englobar outros negócios que não fazem uso desses recursos. A OCDE vira o seu foco para os negócios digitais no seu globo e não apenas para as empresas que usam os dados dos usuários. É, deste modo, que a OCDE integra os dados na solução global e não isola a resposta apenas nos negócios que utilizam os dados dos usuários[32].

E é, em outubro de 2020, então que é lançada a proposta com o objetivo de combater as práticas BEPS, com a intenção de garantir justiça e equidade nos sistemas fiscais, onde os negócios pagam a sua devida parte no local onde geram rendimento, e fortificando o campo fiscal para fazer face aos novos modelos de negócios, e ainda para ajudar os governos a colocarem de volta as suas finanças num caminho sustentável.

---

29 OCDE, *Tax Challenges Arising from Digitalisation – Interim Report 2018: Inclusive Framework on BEPS*. (Disponível em: < https://doi.org/10.1787/9789264293083-en). P.18.

30 E, que já tinham sido identificados no relatório de 2015. OCDE, *Addressing the Tax Challenges of the Digital Economy: Inclusive Framework on BEPS.* (Disponível em: <https://www.oecd.org/tax/addressing-the-tax-challenges-of-the-digital-economy-action-1-2015-final-report-9789264241046-en.htm)

31 *Supra* nota 29.

32 Na verdade, o intuito dos governantes e, conjuntamente, da OCDE é de capturar os rendimentos das multinacionais que devido ao seu tipo de modelo de negócio permite-lhes aceder aos melhores sistemas fiscais de modo a pagarem menos impostos possíveis. Afirme-se já de que, dos modelos de negócios das multinacionais, não se pode afirmar seguramente que há uma ilegalidade, no máximo há uma imoralidade. Porém, as multinacionais não podem ser vistas como as únicas imorais da história, pois grande parte da problemática foi potenciada pelos governos que não conseguiram, e continuam com dificuldades em conseguir, adaptar os seus sistemas fiscais à transformação tecnológica e da economia digital, dando claramente espaço para que as empresas que têm um único objetivo – o lucro – optem por situações mais favoráveis a atingir tal objetivo, não se podendo com isso afirmar que é praticado um ato ilícito.

A proposta inclui dois relatórios, o *Pillar One Blueprint*[33] e *Pillar Two Blueprint*[34], onde se tratam de vários elementos característicos da nova tributação.

De notar que em ambos os relatórios há pontos ainda sob discussão e análise. Muitos em fila de espera para aprovação e acordo entre os países[35]. Por isso, tudo aquilo que se explicará daqui em diante será meramente provisório, sob pena de haver mudanças posteriores à publicação desta investigação, assim, chama-se o leitor à atenção de modificações que existam em momento posterior.

Outro aspeto importante a reter é o facto de que a proposta avante se vira apenas para um número específico de serviços eletrónicos e não para todos os serviços que têm uma atividade na Internet. Portanto, aqui, a OCDE já afunila a sua resposta, afirmando que esta não irá resolver todos os desafios e dar resposta a todas as problemáticas levantadas pela digitalização da economia, e que, por isso, alguns negócios ou atividades podem ficar fora do âmbito da nova proposta, até porque a tentativa de dar uma resposta que abrangesse todos os negócios digitais criaria disrupções e impactos imprevistos na economia digital, podendo mesmo minar a inovação e o desenvolvimento na oferta dos serviços digitais e soluções[36].

Agora, se olharmos atentamente para o relatório de 2018 percebe-se que as grandes atividades que a OCDE e os países pretendem capturar com a nova proposta são as plataformas de redes sociais, a publicidade online e as plataformas de intermediação. Contudo, a proposta abre o seu perímetro para a inclusão de outros negócios.

A proposta, esta alicerça-se em dois pilares, o Pillar One e o Pillar Two.

Superficialmente, o Pillar One procura adaptar o sistema fiscal, através de mudanças no estabelecimento do nexo e nas regras de alocação do lucro, enquanto que o segundo tem como foco uma taxa de imposto mínima global. Ou seja, o primeiro foca-se na atribuição de direitos tributários às jurisdições a partir de um certo montante de receitas residuais e globais de um determinado grupo, ao passo que o segundo olha apenas para o rendimento anual global do grupo para sujeitá-lo a uma taxa mínima global[37].

O Pillar One e o Pillar Two, em conjunto, formam o chamado BEPS 2.0, no entanto, focam-se em questões diferentes. Como este trabalho tem como

---

33 OCDE, *Tax Challenges Arising from Digitalisation – Report on Pillar One Blueprint: Inclusive Framework on BEPS*. (Disponível em: <https://www.oecd.org/tax/beps/tax-challenges-arising-from-digitalisation-report-on-pillar-one-blueprint-beba0634-en.htm>).

34 OCDE, *Tax Challenges Arising from Digitalisation – Report on Pillar Two Blueprint: Inclusive Framework on BEPS.* (Disponível em: <https://www.oecd.org/tax/beps/tax-challenges-arising-from-digitalisation-report-on-pillar-two-blueprint-abb4c3d1-en.htm>).

35 *Supra* nota 33, p.12.

36 *Supra* nota 29, p.184 a 185.

37 Radhakishan Rawal, Madhu Agarwal, *Pillar One and Pillar Two*. (<https://www2.deloitte.com/content/dam/Deloitte/in/Documents/tax/in-tax-pillar-one-and-pillar-two-noexp.pdf>).

objetivo estudar as propostas existentes apenas quanto ao nexo e escopo, então vamo-nos focar daqui em diante somente no Pillar One.

Incidindo no Pillar One, este divide-se em três grandes matérias: o Amount A, o Amount B e a certeza jurídica tributária.

Introduzindo resumidamente o tema, o Amount A traz novas regras sobre a alocação do nexo e do lucro, apresentando um novo direito tributário com uma tributação limitada a um teto de rendimento. Portanto, o Amount A traz novas regras sobre o escopo do novo imposto, i.e., que tipo de atividades e sujeitos serão abrangidos, uma nova regra quanto ao *nexus* que identifica qual a jurisdição legitimada a tributar, tal como regras para determinar o *quantum* de rendimento alocado a uma jurisdição. Há também uma nova abordagem administrativa para a realocação do lucro residual; traz consigo um regime que se desenvolve em paralelo com as despesas, para que não haja tributação deste montante quando o negócio não é rentável ao longo do tempo; apresenta um novo mecanismo de eliminação da dupla tributação (com outro mecanismo complementar que ainda está a ser considerado); introduz um processo administrativo simplificado (com o objetivo de minimizar a complexidade e os custos); e, por fim, traz também consigo algumas mudanças na lei doméstica e uma convenção multilateral[38]. Este modelo está pensado para servir de base para uma futura convenção que, posteriormente, terá de ser transposta para o direito doméstico; portanto, será uma sobreposição ao direito doméstico e ao direito dos tratados[39].

Por sua vez, o Amount B pretende, essencialmente, simplificar o processo administrativo para as autoridades tributárias sobre os preços de transferência e reduzir os custos suportados para os contribuintes. Contudo, este último objetivo é essencialmente direcionado para as atividades de marketing e distribuição (aquelas em que a atividade económica se traduz na compra a uma parte e revenda a terceiros, desde que essa atividade de intermediação seja contínua)[40].

A terceira componente do Pillar One – a certeza jurídica – traz novos mecanismos para a resolução e a prevenção de litígios[41].

Como o nosso foco é no nexo e no escopo, a análise seguirá no âmbito do Amount A. Esta parte do projeto da OCDE fica-se pelo estudo do novo direito tributário, incluindo o nexo e o escopo, que é do que vamos agora em seguida abordar.

Assim sendo, todos os restantes pontos do Pillar One não merecerão interesse da nossa parte (tal como a questão da alocação do rendimento ao

---

38 *Supra* nota 33, p.12 a 14.

39 Jinyan Li, *The Legal Challenges of Creating a Global Tax Regime with the OECD Pillar One Blueprint*. (Disponível em: <http://link.library.ibfd.org/portal/The-legal-challenges-of-creating-a-global-tax/qEVH9CqDUxA/>). P.85.

40 *Supra* nota 33, p..14 a 15

41 *Supra* nota 33, p.15 a 17

território, como a determinação da base tributável, assim como a alocação de lucros, e a eliminação da dupla tributação).

Antes de continuarmos a nossa análise, de forma mais aprofundada, há que alertar o leitor que muitos dos pontos anteriormente mencionados, tais como os subsequentes, ainda estão sob análise e discussão do *Inclusive Framework* da OCDE, por isso, os pontos aqui falados são puramente temporários. Por este exato motivo, ao longo da escrita deste trabalho deparámo-nos com uma mudança significativa quanto ao escopo do novo direito tributário, e desse modo ter-se-á a análise não só do *Pillar One Blueprint* como das novas mudanças.

Se antes, como podemos comprovar pelo relatório sobre o Pillar One[42], fazia-se a distinção entre os *Automated Digital Services* (ADS) e os *Consumer-facing Businesses* (CFB), depois da abertura à opinião pública e ao chamamento de contribuições, o objeto mudou substancialmente[43]. Já quanto ao nexo, este não sofreu muitas mudanças.

Por esta razão, nos subcapítulos seguintes vai-se fazer uma combinação do relatório sobre o Pillar One[44] com o relatório de progresso sobre o Amount A[45].

a) Nexo

Assumindo de antemão que o novo panorama internacional de tributação obriga a uma mudança de paradigma, que não esteja mais exclusivamente dependente de uma presença física, a OCDE, no *Pillar One Blueprint*, propõe novas regras para o estabelecimento do *nexus*, com respeito a todas as atividades e serviços digitais que o próprio Pillar One pretende tributar.

---

42 *Supra* nota 33.

43 Os principais pedidos dos *stakeholders* no comentário ao Pillar One foram, essencialmente, que houvesse uma maior simplificação e a remoção das medidas unilaterais, mudanças no objeto e que fossem providenciadas clarificações sobre como calcular a base tributável no contexto do Amount A. Ainda, ao tempo do relatório várias atividades eram excluídas, o que levou também a apontamentos da opinião externa, que entendeu que algumas atividades que eram incluídas deveriam ser, de igual modo, excluídas. H. Van Dam, C. Kiès, P-A. Klethi, S. Van Der Kroon, J-W. Kunen, B. Farinha Aniceto Da Silva*, International - Taxing the Digitalized Economy: Key Takeaways from the OECD Public Consultation on the Pillar One and Pillar Two Blueprints*. (Disponível em: <http://link.library.ibfd.org/portal/Taxing-the-digitalized-economy--key-takeaways/pggKAvqKXhk/>).

Outro pedido feito pelas demais entidades foi para que o novo direito tributário fosse o mais neutral possível. M Adda, U Lorenzi, F.S. Scandone, *The new taxing right under Pillar One: preliminary thoughts on potential implications for MNEs*. (Disponível em: <http://link.library.ibfd.org/portal/The-new-taxing-right-under-Pillar-One-/rWZJznc7anE/>).

44 *Supra* nota 33.

45 OCDE, *Progress Report On Amount A Of Pillar One - Two-Pillar Solution To The Tax Challenges Of The Digitalisation Of The Economy: Inclusive Framework*. (Disponível em: <https://www.oecd.org/tax/beps/progress-report-on-amount-a-of-pillar-one-two-pillar-solution-to-the-tax-challenges-of-the-digitalisation-of-the-economy.htm>)

O novo elemento constituinte do nexo é: o *quantum* de rendimento anual num determinado mercado seja superior aos limites mínimos que se impõe às empresas cobertas. Será a partir da verificação deste requisito que se entenderá que um determinado Estado estará legitimado a tributar aqueles rendimentos.

O teste do nexo estará satisfeito, quando dentro de certo período de tempo (em princípio de 12 meses) os rendimentos das empresas cobertas pelas regras do objeto e sujeito são iguais ou superiores a 1 milhão de euros. E quando o período tributário for inferior ou superior a 12 meses, o montante é ajustado proporcionalmente de modo a corresponder à duração do período em causa. Quando os rendimentos totais da empresa alocados a determinada jurisdição, num dado período, forem inferiores a 40 bilhões, o montante acima mencionado (de 1 milhão) desce para 250 mil euros.

Para tal contagem só irão ser tidos em conta os rendimentos da entidade do grupo que são cobertos pelas regras do objeto e sujeito, não comportando outras implicações para outra qualquer entidade do grupo[46].

No entanto, pode-se já adiantar (algo que ficará mais completo depois do estudo sobre o objeto da proposta da OCDE) que a proposta da OCDE, apesar de se focar nas atividades que utilizam os dados dos usuários, o seu grande e único intuito é a captura dos rendimentos gerados online que os Estados não conseguem contabilizar segundo as regras atuais de Direito Fiscal Internacional[47].

Apesar disso, bem analisada esta proposta, tecnicamente ela não se foca na tributação dos dados em si mesmos; mas, sim, na tributação dos rendimentos das empresas. Ou seja, o cerne da nova tributação da OCDE não são os dados (e a sua tributação como tal); mas, sim, os rendimentos das empresas (onde os dados são usados como uma âncora para a justificação dessa tributação).

b) Escopo

i. Objeto

Olhando agora para o objeto do novo direito tributário.

Para saber que tipo de atividades estariam no âmbito do novo imposto, o primeiro requisito apontado foi a distinção entre os ADS e/ou os CFB.

Porém, depois da análise da consulta pública, a OCDE decidiu retirar estas duas categorias, por, essencialmente, achar demasiado complexa a distinção.

No novo relatório[48] já mais conciso sobre o Amount A, também se desiste da inclusão de algumas atividades anteriormente pensadas, tal como, por

46 *Supra* nota 54, p.13.
47 *Supra* nota 8.
48 *Supra* nota 45.

outro lado, se passou a incluir outras. Como este último documento publicado pela OCDE não inclui uma breve definição das atividades, como aconteceu no relatório *Blueprint*, apenas se ficando por uma breve referência ao que se considera incluído em cada uma, então utilizar-se-ão as definições dadas no *Blueprint* para aquelas atividades que continuam a fazer parte do objeto no relatório de progresso.

Começando pela enumeração dos serviços compreendidos pela incidência objetiva, fazem parte da nova lista: os serviços localmente especificados; os serviços de publicidade (online); a venda, licenciamento ou outra alienação de propriedade intangível e dos dados dos usuários; os serviços de transporte; serviços de intermediação online; programas de recompensa do cliente; alienação de propriedade real; subsídios do governo; e outros serviços[49].

De seguida, e tendo em conta o foco do trabalho, apenas se vai fazer a análise nos serviços que estão diretamente relacionados com os dados dos utilizadores[50].

Primeiramente, os serviços de publicidade online, segundo a definição dada pela OCDE[51], serão todos aqueles em que há um serviço online que coloca publicidade numa interface digital. Na definição também estarão incluídos todos os sistemas vocacionados para a atracão de potenciais visualizadores dos anúncios, tais como aqueles que recolhem dados e as contribuições dos indivíduos, por via de acesso a uma interface digital, como os motores de busca, as plataformas de redes sociais ou os serviços de conteúdo digital.

O que se pretende captar com esta medida são todas as receitas que advêm dos pagamentos para serviços de publicidade online. Fala-se aqui das situações em que uma empresa pretende disponibilizar determinado anúncio num local da Internet e, para isso, paga um *quantum* para poder colocar o tal anúncio na interface digital. Mas, para tornar estes serviços mais rentáveis e personalizados, as interfaces digitais recolhem os dados dos usuários, dados recolhidos por e gerados nessas interfaces que permitem saber o que lhes poderá interessar e, posteriormente, direcionar a publicidade de bens e serviços no seguimento dos interesses dos usuários, a partir da disponibilização dos dados por estes.

---

49 Os serviços não estão em departamentos estanques, podendo muitas vezes misturarem-se (por ex., um serviço de publicidade online pode também vender os dados dos usuários que coleta).

50 Pelo que para um maior aprofundamento remete-se o leitor para a leitura do relatório *Supra* nota 45, p.64 a 82.

51 O texto original da proposta da OCDE no relatório *Blueprint* é: *"This means online services aimed at placing advertisement on a digital interface, including services for the purchase, storage and distribution of advertising messages, and for advertising monitoring and performance measurement. It includes related systems for attracting potential viewers of the advertisements and collecting content contributions from them and data regarding them, including via the provision of access to a digital interface, such as search engines, social media platforms or digital content services. Supra* nota 33, p.25.

Como foi explicado pela OCDE no comentário à definição destes serviços, estarão incluídos nesta definição todos os serviços de publicidade direta, tais como as plataformas de redes sociais, motores de busca online, plataformas de intermediação online e serviços de conteúdo digital que vendem diretamente inventários de publicidade para exibição nas interfaces digitais em que operam. A definição também se alarga, através da expressão "*digital interface*", a todos os serviços de publicidade online exibidos também em aparelhos que estejam conectados à Internet ("*Internet of Things*").

Portanto, estes serviços apesar de não incidirem diretamente sobre os dados dos utilizadores, permitem que os dados representem aqui um papel fulcral, pois os operadores os recolhem e os estudam a partir dos utilizadores, para prestarem serviços de publicidade muito mais personalizados e daí obterem um maior rendimento. Ora, então, os dados são deveras importantes, pois sem estes os serviços não seriam tão rentáveis para as empresas.

Em segundo lugar, a OCDE[52] pretende tributar os rendimentos que advêm da venda, ou licenciamento a um terceiro acerca dos dados dos utilizadores e dados gerados por estes no uso de uma interface digital.

No comentário é mesmo reconhecido que o que se pretende tributar com a inclusão desta definição são os modelos de negócios que monitorizam os dados dos usuários gerados numa interface digital, para depois vender, licenciar ou alienar por outro meio a terceiros.

A intenção será o de abranger o maior número de casos possível, facto pelo qual a definição de interface digital deve ser o mais abrangente possível, incluindo também as interfaces que estão conectadas com a Internet num bem físico (i.e., *"Internet of Things"*).

Já os dados dos usuários a que a OCDE se refere são todos aqueles que incluem informações sobre os seus proprietários, tais como os seus hábitos, despesas, localização, ambiente, uso de serviços, *hobbies*, ou interesses pessoais, incluindo dados agregados e anónimos (como por ex., informação da geolocalização e os níveis de trânsito). No entanto, é possível que este pacote seja ainda estendido aos dados industriais, científicos, estatísticos, ou outros não conectados com pessoas (como os negócios que adquirem e disseminam informações sobre investimentos e mercados financeiros, ou para investigação científica), contudo estes serviços já poderiam estar sob a alçada dos serviços de conteúdo digital, onde são providenciados os dados de forma automatizada, como as bases de dados ou librarias online.

Porém, os dados devem ser recolhidos pela própria empresa como dados puros, i.e., sem nenhum tratamento (por ex., o vendedor de um sistema de aquecimento de casas acede aos dados sobre o uso da energia, ou uma pla-

[52] Texto original da proposta da OCDE no relatório *Blueprint: "This means selling, licensing or otherwise alienating to an unrelated third party customer user data generated by users of a digital interface.". Supra* nota 33, p.26.

taforma de rede social recolhe os dados sobre os usuários), ou devem ser adquiridos a outra empresa.

Outra definição que aqui interessa abordar é a questão das plataformas de redes sociais[53]. No entendimento da OCDE, configurarão este tipo de serviços todas as plataformas disponibilizadas numa interface digital, a qual facilita a interação entre os usuários, ou entre estes e o conteúdo gerado pelos mesmos[54].

Então, incluir-se-á nesta categoria todas as atividades que dependem ativamente dos usuários para a criação de valor. São os casos das plataformas sociais e de *networking* profissional, os microblogues, plataformas de partilha de vídeos e imagens, de online *dating*, plataformas dedicadas à partilha de avaliações por parte dos utilizadores, mas também as plataformas de chamadas e mensagens online. Mais uma vez, estas categorias não são estanques, pelo que muitas plataformas praticam mais do que um serviço acima enumerado.

Também estarão incluídas na definição de plataformas de redes sociais, aquelas que oferecem o acesso aos usuários mediante um pagamento, por ex., de uma subscrição. Mas já não estão incluídas aquelas plataformas em que a interação dos usuários é meramente incidental e não representa sequer o principal propósito da interface digital (no comentário desenvolvido pela OCDE é dado o exemplo de uma empresa que vende o seu próprio inventário online e o seu *website* permite aos usuários colocarem comentários ou avaliações).

Assim, mais uma vez, os serviços acima enunciados podem misturar-se com outras categorias. Muitas das atividades caem na definição da plataforma de redes sociais são muitas vezes financiadas através dos serviços de publicidade online, pela venda de dados ou por subscrições, e quando assim o é, o lucro deve ser tratado sob a alçada de cada uma das respetivas categorias.

Após a análise do objeto do novo direito tributário pode-se afirmar com grande veemência que a maior parte dos negócios que a OCDE tenta com este novo direito tributar, só ocorrem, maioritariamente, pela colheita dos dados dos usuários, estudo para vender, licenciar ou utilizar para a venda de outro serviço (no caso, por ex., dos serviços de publicidade).

Há ainda que referir que não há, para já, um consenso entre os países do *Inclusive Framework* sobre as várias categorias nem a sua extensão. O prin-

---

53 De salientar que esta categoria não aparece expressamente no novo relatório, mas pensa-se que se poderá incluir na categoria dos serviços localmente especificados, onde também se compreendem os serviços conectados com uma propriedade tangível. Quer-se aqui incluir definitivamente os serviços de *"Internet of Things",* mas também, poder-se-á considerar abrangidas as plataformas digitais que são acedidas através de um aparelho eletrónico também.

54 O texto original da proposta da OCDE no *Blueprint* é: *"This means making a platform available on a digital interface to facilitate the interaction between users or between users and user-generated content". Supra* nota 33, p.27.

cipal desafio para o Direito Fiscal Internacional, para lá do da digitalização da economia, são as forças políticas dos vários países, o que torna difícil (mas não impossível) chegar a um acordo multilateral.

ii. Sujeito

Na temática do sujeito, i.e., saber que empresas serão vítimas do novo direito tributário, a OCDE divide as empresas em duas categorias: o grupo coberto e o grupo excluído.

Para determinar quem faz parte do grupo coberto pelo novo imposto, contarão os rendimentos que certa empresa tenha num dado período de tempo. E, para tal afunilamento, a OCDE baseia-se em dois testes: o teste do rendimento (*the revenue test*) e um teste de rentabilidade (*the profitability test*).

Ora, um grupo é considerado abrangido pelo escopo do imposto, quando: (1) o montante dos rendimentos globais do grupo durante o período tributário (em princípio de 12 meses) ultrapassarem os 20 biliões[55] (teste do rendimento) – mas quando o período é inferior ou maior que os 12 meses, o valor é ajustado proporcionalmente à duração do período -; (2) e, quando a margem de lucro pré-imposto do grupo for superior a 10% (teste de rentabilidade). Passar-se-á no teste da rentabilidade quando o lucro do grupo coberto ultrapassar o limite dos 10% num dado período (teste do período ou *the period test*), e quando o seu lucro ultrapassar o limite dos 10% em pelo menos dois períodos dos quatro imediatamente anteriores ao período tributário em causa (*the prior period test*), e esse limite for excedido em média durante o período em questão e nos quatro períodos imediatamente anteriores (*the average test*)[56][57].

Na categoria das atividades excluídas estarão o grupo dos extrativos qualificados e os serviços financeiros regulamentados. O primeiro grupo engloba as atividades de exploração, desenvolvimento e extração, desde que tenham rendimentos derivados dessa atividade de exploração, desenvolvi-

---

55 Umas das críticas apontadas pelas partes intervenientes na consulta pública do Pillar One foi a utilização do Euro como a moeda preterida. Surgiram dúvidas sobre como os países e as empresas que não lidam com o Euro vão conseguir fazer a conversão, com os problemas de flutuações presentes. A *WU Transfer Pricing Center at the Institute for Austrian and International Tax Law at Vienna University of Economics and Business* não ficou convencida de que o limite deve ser limitado a apenas uma moeda, tendo em conta as incertezas socioeconómicas globais. Para tal, a Universidade sugere que a OCDE considere adicionar e permitir outras moedas ou então que determine como as companhias devem ultrapassar as flutuações na conversão entre moedas. Nana Sarfo, *Stakeholders' Deep Dive Into Amount A In-Scope Rules*. (Disponível em: <https://www.taxnotes.com/tax-notes-today-international/international-taxation/stakeholders-deep-dive-amount-scope-rules/2022/05/23/7dhnj>).

56 *Supra* nota 45, p.10 a 11.

57 *Supra* nota 55.

mento ou extração[58]. No âmbito da segunda categoria, estará fora do escopo o grupo do qual uma ou mais entidades parentes são instituições de depósitos, de crédito, de investimento, de seguros, de gestão de ativos, de financiamento misto ou de serviços de pedidos de informação[59]. Estarão assim excluídos estes grupos do escopo, exceto se se verificarem os testes do não-rendimento e da não-rentabilidade definidos para cada uma das categorias.

Apesar da proposta, como tal, ainda não há qualquer veredicto sobre o *quantum* a partir do qual uma empresa passa a estar abrangida. E, muitas mudanças ainda são esperadas no âmbito do escopo, sob pena de não haver uma adesão em massa de ambas as partes, dos países e das companhias afetadas.

3.2. DIREITO COMPARADO

Desde 2015 que a OCDE tenta solucionar a complexa questão da economia digital para auxiliar os países a adaptarem os seus regimes fiscais aos desafios trazidos pela digitalização. Porém, enquanto essa solução não se torna possível e efetiva, alguns países foram já implementando algumas medidas no sentido de tributar os dados, no limiar das suas jurisdições.

Esta ânsia surgiu pela perceção que alguns governos tiveram da quantidade de rendimento gerado nas suas jurisdições, onde estavam a "perder". Perder, pois, caso fosse o mercado de dados tributado, os governos conseguiriam arrecadar milhões em receita. E, como a solução da OCDE tem um longo caminho pela frente, sem certeza de quando será a sua implementação, e se irá existir, alguns países foram começando a arranjar formas de iniciar a tributação do mercado de dados.

Este capítulo vai-se focar exatamente nas respostas individuais que cada país foi dando para tributar o mercado de dados.

Não obstante, este estudo apenas se irá debruçar sobre alguns países que, digamos, estão na vanguarda da evolução deste tipo de tributação. Mas apenas nos iremos focar na análise sobre três dos elementos das propostas de tributação: o nexo, o objeto e o sujeito.

De realçar que, a 21 de outubro de 2021, a Áustria, França, Itália, Espanha, Reino Unido e EUA assinaram um acordo – o *Unilateral Measures Compromise* – no qual se determina um sistema transicional que permite aos signatários aplicarem medidas unilaterais para a tributação da economia digital durante o período que antecede a reforma internacional no âmbito fiscal, ou seja, enquanto não é implementado o Pillar One, desenvolvido pela OCDE no projeto Two-Pillar[60]

---

58 Para maior aprofundamento ver *Supra* nota 45, p.44 a 46.

59 Para maior aprofundamento ver *Supra* nota 45, p.46 a 58.

60 Diploma disponível em: https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=5EEE687F-D512-475B-B940-F85237E00E1C&filename=1575%20-%20Joint%20Statement%20on%20unilateral%20measures.pdf

a) Áustria[61]

Em 1 de janeiro de 2020 entra em vigor o *Digitalsteuergesetz 2020* (DiStG 2020)[62]. Esta legislação introduz um novo imposto – o DST (*Digital Service Tax*).

Este imposto visa apenas tributar os serviços de publicidade online providenciados pelos "*digital service providers*", i.e., as companhias que oferecem serviços digitais, independentemente de serem residentes ou não no país[63].

Contudo, só tem relevância para a tributação a publicidade online que é providenciada domesticamente e que, nos termos da legislação, acontece quando a publicidade é recebida por um aparelho eletrónico, onde tem um endereço de IP doméstico, e ainda quando o conteúdo e o *design* são direcionados para utilizadores domésticos.

b) Brasil[64]

O Brasil, de entre as várias jurisdições que estão na vanguarda da tributação da economia digital, foi o país que mais propostas apresentou.

No total, são quatro as propostas que fazem parte do pacote de adaptação do sistema fiscal à digitalização da economia. São elas: a CIDE-digital, a Contribuição Social sobre Serviços Digitais (CSSD), a Contribuição sobre Bens e Serviços (CBS) e a Contribuição para o Financiamento da Seguridade Social (COFINS-digital).

A CIDE-digital dispõe que as empresas (residentes ou não) que tenham um rendimento anual global de pelo menos 3 biliões e um rendimento doméstico de pelo menos 100 milhões de reais passem a ser tributadas num espectro entre 1 a 5%, dependendo do montante de rendimento.

Contudo, só são contabilizadas (i.e., o objeto da tributação) as atividades em que o rendimento advém de serviços de publicidade online para usuários localizados no Brasil; em que há a disponibilização de plataformas digitais que permitem aos usuários interagir entre si e vender bens ou prestar serviços entre si, sempre que pelo menos um dos usuários está localizado no Brasil; e, ainda, quando há a transmissão de dados de utilizadores localizados no Brasil, os quais foram gerados por si mesmos ou recolhidos enquanto faziam uso de uma plataforma digital.

A par da proposta desenvolvida pelas autoridades brasileiras para a tributação das multinacionais digitais, estão a CBS, a COFINS-digital e a CSSD.

---

61 IBFD, Austria - Digital Taxation Monitor. Disponível em: https://research.ibfd.org/#/doc?url=/linkresolver/static/dtm_at)

62 Diploma disponível em: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010780

63 Y. Schuchter & A. Kras, *Austria - Corporate Taxation. Country Tax Guides IBFD*. Disponível em: https://research.ibfd.org/#/doc?url=/document/cta_at_s_14.

64 Diploma disponível em: https://research.ibfd.org/#/doc?url=/document/dtm_br

A primeira, *Contribution on goods and services* (CBS), com o nome original de "Contribuição sobre Bens e Serviços (CBS)"[65], pretende tributar o rendimento bruto de importação e vendas locais de serviços e mercadorias das entidades que prestem serviços e vendam mercadorias, inclusive entidades não residentes em caso de importação[66].

Já a segunda, com o nome original "Contribuição para o Financiamento da Seguridade Social (COFINS-digital)"[67], constitui uma tributação para financiar a segurança social. Quem deverá contribuir serão todas as entidades legais que façam uso das plataformas digitais para: 1) através de canais eletrónicos oferecerem uma interface digital que permite aos usuários contactarem e interagirem entre si, com o objetivo de entregarem bens ou prestarem serviços, e 2) serviços de marketing para anunciantes ou para os seus agentes, disponibilizando mensagens publicitárias direcionadas aos utilizadores numa interface digital com base nos dados desses. Assim, todas as entidades residentes ou não residentes, com um rendimento bruto advindo daqueles serviços digitais providenciados mundialmente, que excedam 20 milhões, e no Brasil excedam 6,5 milhões de reais, estarão sujeitas a este tributo.

A *Social Contribution on digital Services* (CSSD), com o nome original "Contribuição Social sobre Serviços Digitais incidente sobre a receita bruta de serviços digitais prestados pelas grandes empresas de tecnologia (CSSD)"[68], por sua vez, pretende tributar os rendimentos advindos: 1) da exibição de anúncios em plataforma digitais para usuários localizados no Brasil; 2) da disponibilização de plataformas digitais que permitam aos usuários contactar e interagir entre si para fins de venda de bens ou prestação de serviços diretamente entre si, desde que um dos usuários esteja localizado no Brasil; 3) da transmissão de dados de usuários localizados no Brasil, que tenham sido recolhidos durante o uso das plataformas digitais ou gerados por esses usuários. Portanto, todas as empresas residentes e não residentes, que obtenham um rendimento no Brasil e pertençam a um grupo económico que tenha contabilizado no ano anterior um rendimento global equivalente ou superior a 4,5 biliões de reais, achar-se-ão abrangidas por este tributo.

É de extrema importância referir que para as propostas apresentadas pelo Brasil, e também por outros países, não é dada importância ao princípio da nacionalidade, apenas ao da territorialidade, visto que não é necessário ser uma empresa residente ou não no Brasil. O elemento de conexão ao território passa apenas pela oferta de espaços digitais a usuários que

---

[65] Diploma disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2258196

[66] IBFD - Brazil - Digital Taxation Monitor. Disponível em: https://research.ibfd.org/#/doc?url=/document/dtm_br

[67] Diploma disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/142074

[68] Diploma disponível em:: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2260638

esses, sim, têm de estar localizados no território brasileiro. E, para tal efeito, serão considerados usuários localizados no Brasil aqueles que acedam às plataformas digitais em aparelhos eletrónicos que estão localizados nesse país. Ou seja, para o legislador fiscal brasileiro não importa nem a nacionalidade das empresas, nem sequer a nacionalidade dos sujeitos, apenas importa onde estão localizados os aparelhos através dos quais acedem às plataformas digitais.

Esta forma de pensamento, que transfere o nexo de ligação ao território do sujeito *per se* para o aparelho eletrónico, é uma inovação para o Direito Fiscal em que o sujeito deixa de ser importante para o estabelecimento do nexo.

c) Espanha[69]

No caso de Espanha, o DST entrou em vigor a 16 de janeiro de 2021, com o nome de *Impuesto sobre Determinados Servicios Digitales*[70].

O novo imposto espanhol destina-se às empresas que providenciem serviços de publicidade online, serviços de intermediação online, e que transmitam dados gerados pelos usuários no uso das interfaces digitais (seja em venda ou concessão)[71].

d) França[72]

Em França, desde 1 de janeiro de 2019 que está implantado o DST - *Taxe sur certains services fournis par les grandes entreprises du secteur numérique* (TSN)[73].

São sujeitas ao imposto todas as empresas, residentes ou não, que ofereçam interfaces digitais (serviços de intermediação), coloquem numa interface digital publicidade online direcionada para os utilizadores dessa mesma interface, e/ou que transmitam os dados que foram produzidos pelos usuários no uso das plataformas digitais[74].

A inovação desta solução prende-se na forma do cálculo da base tributável: o volume de negócios com origem no território francês é calculado usando um coeficiente de presença digital baseado na proporção de usuários franceses.

---

69 IBFD - Spain - Digital Taxation Monitor. Disponível em: https://research.ibfd.org/#/doc?url=/document/dtm_es

70 Diploma disponível em: https://www.boe.es/boe/dias/2020/10/16/pdfs/BOE-A-2020-12355.pdf

71 Á. De La Cueva González-Cotera & A. Arroyo Ataz, *Spain - Corporate Taxation*. Documento disponível em: https://research.ibfd.org/#/doc?url=/document/cta_es_s_14.

72 IBFD - France - Digital Taxation Monitor. Disponível em: https://research.ibfd.org/#/doc?url=/document/dtm_fr

73 Diploma disponível em: https://www.impots.gouv.fr/sites/default/files/media/1_metier/5_international/french_dst_en_v2.pdf?l=en

74 P. Burg, *France - Corporate Taxation*. Disponível em: https://research.ibfd.org/#/doc?url=/document/cta_fr_s_14.

e) Hungria[75]

Já a Hungria, desde 15 de agosto de 2014, implementa, no contexto digital, um imposto sobre a publicidade – o *Reklámadó*[76].

Este nada mais é do que um imposto sobre empresas, residentes ou não residentes, que vendem tempo ou espaço nas plataformas digitais para publicidade, para os media e para a imprensa[77].

f) Índia[78]

Na Índia vigoram três tipos de tributação sobre as interfaces digitais.

Desde 1 de junho de 2016 que vigora o *Equalisation Levy* (EL)[79], destinado aos serviços de publicidade online, serviços de oferta de espaço ou outra qualquer facilidade para prestação de publicidade online, ou serviços de publicidade online prestados por não residentes. Contudo, em 1 de abril de 2020, o seu âmbito foi alargado à venda de bens e prestação de serviços online por parte de operadores de comércio eletrónico[80].

A par deste, o legislador tributário indiano aplica ainda o *Income Tax (on significant economic presence - SEP).* O conceito de presença económica significativa (numa dada jurisdição) é o novo elemento de estabelecimento do nexo. Apesar de este imposto não ter em mente a tributação direta das interfaces digitais, o operador económico (que até pode ter uma atividade digital que não cai no âmbito da EL) passará a ser considerado sujeito tributário sob o *Income Tax*, a partir do momento em que se prove que tem rendimentos e uma presença económica significativa no mercado nacional.

g) Indonésia[81]

Apesar de algumas evoluções na discussão sobre a implementação de uma tributação na economia digital, é certo que ainda nenhuma medida foi implementada, apesar de já ter sido aprovada.

---

75 IBFD - Hungary - Digital Taxation Monitor. Disponível em: https://research.ibfd.org/#/doc?url=/document/dtm_hu

76 Diploma disponível em: https://net.jogtar.hu/jogszabaly?docid=a1400022.tv

77 G. ErdőS, *Hungary - Corporate Taxation*. Disponível em: https://research.ibfd.org/#/doc?url=/document/cta_hu_s_14.

78 IBFD - India - Digital Taxation Monitor. Disponível em: https://research.ibfd.org/#/doc?url=/document/dtm_in

79 Diploma disponível em: https://www.incometaxindia.gov.in/pages/acts/equalisation-levy.aspx

80 S. Shah, *India - Corporate Taxation*. Disponível em: https://research.ibfd.org/#/doc?url=/document/cta_in_s_2.

81 IBFD - Indonesia - Digital Taxation Monitor. Disponível em: https://research.ibfd.org/#/doc?url=/document/dtm_id

O que está sobre a mesa é o *Pajak Penghasilan,* através do qual todas as atividades de comércio eletrónico providenciadas por operadores estrangeiros passarão a ser tributadas, desde que apresentem uma presença económica significativa na Indonésia.

h) Itália[82]

Tal como os restantes países europeus já mencionados anteriormente, Itália também implementou um DST – o *Imposta sui Servizi Digitali* – a 1 de janeiro de 2020, através do qual passaram a estar sujeitas àquela tributação as empresas, residentes ou não residentes, que providenciem serviços digitais[83]. Os serviços abrangidos por este novo imposto são os mesmos tributados pela França, como referidos anteriormente, e para aí se remete o leitor.

A par desta tributação, tal como a Índia, a Itália aplica ainda um *Income Tax (on significant economic presence - SEP)* – o *Imposta sul Reddito delle Società.*

i) Quénia

A implementação no Quénia de um DST[84] deu-se a 1 de janeiro de 2021.

Este novo imposto aplica-se ao provisionamento dos seguintes serviços: conteúdo digital para download, incluindo aplicativos móveis para download, e-books e filmes; serviços *over-the-top*, incluindo *streaming* de programas de televisão, filmes, música, *podcasts* e qualquer forma de conteúdo digital; venda, licenciamento ou qualquer outra forma de monetização de dados recolhidos dos usuários quenianos que foram gerados a partir das atividades dos usuários no mercado digital; o provisionamento de um mercado digital; os media baseados em assinatura, incluindo notícias, revistas e jornais; gerenciamento eletrónico de dados, incluindo hospedagem de *websites*, armazenamento de dados on-line, compartilhamento de arquivos e serviços de armazenamento em nuvem; serviços de reserva eletrónica ou de bilheteira eletrónica, incluindo a venda online de bilhetes; fornecimento de motores de busca e serviços automatizados de receção, incluindo o fornecimento de serviços personalizados de motores de busca; ensino à distância por meio de pré-gravação ou *e-learning*, incluindo cursos e treinos online; e qualquer outro serviço prestado através de um mercado digital. Estão isentos os serviços online prestados por instituições financeiras e prestadores de serviços financeiros aprovados para facilitar pagamentos, empréstimos

82 IBFD - Italy - Digital Taxation Monitor. Disponível em: https://research.ibfd.org/#/doc?url=/document/dtm_it

83 C. (Cesare) Silvani, *Italy - Corporate Taxation*. Disponível em: https://research.ibfd.org/#/doc?url=/document/cta_it_s_14.

84 Diploma disponível em: http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=CAP.%20470#part_II e a Bill relativa a 2022 http://www.parliament.go.ke/sites/default/files/2022-04/The%20Finance%20Bill%2C%202022-1.pdf

ou negociação de instrumentos financeiros, mercadorias ou câmbio, bem como serviços online prestados por instituições governamentais.

Mas, só estarão sujeitos a este novo imposto, os sujeitos não residentes, cujos rendimentos que resultam da prestação de serviços, são derivados ou acumulados no Quênia por meio de um negócio realizado pela Internet, ou por uma rede eletrónica, inclusive por meio de um mercado digital. "Mercado digital", neste contexto legislativo, significará uma plataforma online ou eletrónica que permite aos usuários venderem bens ou prestarem serviços entre si. Aplicar-se-á também a residentes que prestaram serviços sujeitos a DST entre janeiro e junho de 2020 (antes da Lei das Finanças de 2021 que alterou a Lei do Imposto sobre o Rendimento que isenta os residentes de DST)[85].

j) Reino unido (RU)

No Reino Unido, entrou *in force* a 1 de abril de 2020 um DST[86].

As pessoas tributadas por este instrumento legislativo serão todas as empresas residentes e não residentes com volume de negócios mundial (em nível consolidado) pela prestação de serviços, que são por si tributáveis, superiores a 500 milhões de libras, com pelo menos 25 milhões de livras dessas receitas provenientes de usuários estabelecidos no Reino Unido, pela provisão de uma plataforma de redes sociais, mecanismo de pesquisa na Internet ou um mercado online para usuários no Reino Unido[87].

k) Turquia[88]

A 1 de Março de 2020 entra em força também um DST (com o nome original de "*Dijital Hizmet Vergisi").* Segundo os seus termos legislativos, estarão sujeitas a este imposto todas as empresas e indivíduos, residentes e não residentes, pela prestação de serviços que são sujeitos a tributação, que geram um volume de negócios mundial superior a 750 milhões de euros e um volume de negócios na Turquia superior a 20 milhões de liras turcas. São considerados serviços digitais para este efeito todos os tipos de serviços de publicidade online (incluindo serviços de controlo de publicidade e medição de desempenho, serviços relacionados à transmissão e gerenciamento de dados do usuário e serviços técnicos relacionados à apresentação de anúncios); a venda de áudio, vídeo ou qualquer conteúdo digital; quaisquer

---

85 IBFD - Kenya - Digital Taxation Monitor. Disponível em: https://research.ibfd.org/#/doc?url=/document/dtm_ke

86 Diploma disponível em: https://www.legislation.gov.uk/ukpga/2020/14/part/2/enacted, https://www.gov.uk/hmrc-internal-manuals/digital-services-tax, https://www.legislation.gov.uk/ukpga/2020/14/schedule/8/enacted

87 IBFD – United Kingdom - Digital Taxation Monitor. Disponível em: https://research.ibfd.org/#/doc?url=/document/dtm_uk

88 IBFD - Turkey- Digital Taxation Monitor. Disponível em: https://research.ibfd.org/#/doc?url=/document/dtm_tr

serviços realizados em ambiente digital que possibilitem que os conteúdos sejam ouvidos, assistidos e/ou reproduzidos digitalmente; o áudio, vídeo ou qualquer conteúdo digital gravado ou usado em dispositivos eletrónicos; a prestação e gestão de serviços online que permitem aos utilizadores interagir entre si (incluindo serviços que são realizados para permitir ou facilitar a venda de bens ou serviços entre utilizadores); e os serviços de intermediação realizados em ambiente digital relativos aos serviços acima mencionados.

Contudo, a par deste novo imposto, a Turquia decidiu paralelamente tributar os serviços de publicidade online, para qualquer residente e não residente que preste serviços de publicidade e intermediação para a prestação de serviços de publicidade através da Internet[89].

l) União Europeia (UE)[90]

A UE, não diferentemente da tendência, tem estudado um pacote de propostas para dar resposta à tributação da economia digital.

Na vanguarda, está a mais importante: a tributação dos serviços digitais (um DST)[91]. Sob esta proposta estarão incluídos todos os serviços de publicidade online, a venda de dados pessoais com o destino de publicidade e a intermediação de serviços. E sob tal, serão afetadas todas as entidades com rendimentos totais anuais superiores a 750 milhões de euros e rendimentos cumulativos na UE superiores a 50 milhões de euros.

Paralelamente, também ainda em estado de análise, a UE propôs um imposto sobre o rendimento das pessoas coletivas, que irá depender da taxa de IRC dos Estados-Membros para quando houver uma presença digital significativa (o chamado *Corporate of an Significant Digital Presence* – SDP)[92]. No escopo estarão as pessoas coletivas incorporadas ou estabelecidas na UE e as não residentes com uma presença digital significativa no espaço da UE, que tenham rendas atribuídas à tal presença digital num Estado-Membro superiores a 7 milhões de euros num ano, 100 mil usuários ou 3 mil contratos de negócios para serviços digitais num Estado-Membro. Por serviços digitais entender-se-á os serviços que são disponibilizados via Internet ou de uma rede eletrónica, cuja natureza faz com que o serviço seja totalmente automatizado (i.e., a prestação do serviço sem o recurso à tecnologia de informação é impossível) envolvendo a mínima intervenção humana.

---

89 Diploma disponível em: https://www.resmigazete.gov.tr/eskiler/2022/05/20220531-7.htm

90 IBFD – European Union - Digital Taxation Monitor. Disponível em: https://research.ibfd.org/#/doc?url=/document/dtm_e2

91 Diploma disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A148%3AFIN

92 Diploma disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018PC0147

Uma outra novidade foi a proposta da UE para a introdução de uma taxa digital (*digital levy*). Este tributo, que será, em princípio, sobre o rendimento ou sobre as transações digitais, destina-se às companhias que pratiquem certas atividades digitais. Entrando em vigor, não se vai sobrepor à proposta da OCDE, pois esta está pensada para ser compatível com o acordo internacional que seja celebrado ao nível deste organismo.

Ainda faz parte do conjunto, uma proposta de diretiva[93] que deve ser transposta e deve entrar em vigor a 1 de janeiro de 2023. Esta determina que as operadoras de plataformas, que presentes na UE, sejam residentes, incorporadas, geridas, ou têm um EE num Estado-Membro, ou até aquelas não residentes na UE, terão de reportar as atividades que envolvam o arrendamento de bens imóveis, serviços pessoais, venda de bens e o arrendamento de qualquer meio de transporte. As plataformas terão de prestar as identificações dos vendedores, determinar o Estado-Membro da residência do vendedor e, quando aplicável, providenciar as informações sobre o arrendamento dos seus bens imóveis. Para além disso, terão, obviamente, de fornecer informações sobre si, sobre as suas contas bancárias e os respetivos detentores, os pagamentos aos vendedores, e as taxas ou impostos cobrados.

Como foi referido, nenhuma das propostas levada a cabo pela UE está em vigor. Enquanto as duas primeiras estão sob análise e estudo, esperando pelos comentários da consulta pública ou que haja um acordo internacional ao nível da OCDE, a última proposta referida entrará em vigor, em princípio, em 2023; mas dependerá, sendo uma diretiva, da transposição dos Estados-Membros.

m) Estados Unidos da América (EUA)[94]

A maior parte das multinacionais com as maiores presenças digitais estão sediadas nos EUA. Com receio de ser profundamente afetado, os EUA decidiram iniciar uma investigação a todos os países anteriormente mencionados e à UE, com exceção do Brasil, República Checa e Indonésia, onde esta investigação está suspensa apenas pelo facto de estes três países ainda não terem implementado efetivamente uma tributação digital.

Os EUA não impõem um imposto federal direto sobre a economia digitalizada. No entanto, vários dos seus Estados tributam produtos e serviços digitais de acordo com seus regimes de impostos sobre vendas ou sobre rendimentos brutos (isto inclui (1) imposto sobre a venda de um produto ou serviço digital; e (2) imposto sobre a licença ou assinatura para uso tal produto ou serviço digital).

---

93 Disponível em: https://research.ibfd.org/#/doc?url=/linkresolver/static/tt_e2_41_eng_2011_tt__ad7%23tt_e2_41_eng_2011_tt__ad7

94 IBFD – United States - Digital Taxation Monitor. Disponível em: https://research.ibfd.org/#/doc?url=/document/dtm_us

Maryland é o único Estado dos EUA a promulgar oficialmente um imposto de serviço digital separado (que entrou em vigor a partir de 1 de janeiro de 2022) que incidirá sobre os contribuintes com pelo menos US$ 100 milhões em receitas anuais globais, onde pelo menos 1 milhão de dólares das receitas são provenientes de Maryland.

4. TRIBUTAÇÃO DE DADOS

Como se viu até agora, a tributação da economia digital é uma matéria em destaque nas agendas dos governos e em Direito Fiscal Internacional.

A controvérsia envolta é complexa e mesmo entre os fiscalistas há pontos de discórdia e diferentes perspetivas de como tributar os vários serviços e atividades digitais. A complexidade ganha outros contornos, quando a questão se restringe à tributação dos dados pessoais *per se*.

De entre vários temas que se irão discutir sobre a matéria, iremos apenas nos debruçar no nexo, objeto e sujeito da possível via para a tributação de dados.

Como visto até aqui, os dados permitem tanto a existência como o funcionamento da economia digital. Muitos dos novos modelos de negócios nascidos com a economia digital baseiam-se na recolha e/ou tratamento dos dados dos usuários, como o *core* do próprio negócio, ou como uma atividade secundária que alimenta a principal.

Portanto, os consumidores criam valor pela provisão dos seus dados pessoais (ou a permissão da sua recolha) e pela criação de conteúdo digital, que podem ser ambos monetizados pelas empresas, mas também pela via da criação de uma rede de *network*[95].

Neste prisma a reflexão intuitiva é: se os dados dos consumidores contribuem para a possível valorização da empresa ou geram receita para a mesma, então porque não os tributar? Assim, apesar de ser atrativo cairmos neste pensamento, tem de se chamar a atenção que o tema é mais complexo do que aquilo que possa parecer.

Mesmo o Fundo Monetário Internacional (FMI) levanta questões de como os dados devem ser tributados. Devem os usuários ser remunerados diretamente e, posteriormente, taxados em sede de IRS, enquanto a remuneração é dedutível em sede de IRC para a empresa? Ou os governos deveriam tributar uma porção dos lucros dos negócios digitais, servindo de intermédio e em nome dos usuários? Por outras palavras, deve o valor gerado pelo usuário estabelecer direitos de tributação para baseados na fonte para o país em que os usuários residem?[96]

---

95 *Supra* nota 1, p.7 a 8.

96 *Supra* nota 1, p.11.

Para começar, tem de se ter em mente que muito do Direito Fiscal é desenhado dependendo da vontade política. Portanto, qualquer que seja a solução adotada será com base não só na ideologia, como também nas ambições e posições políticas dos vários países.

As razões por detrás de uma nova tributação podem ser variadas. E, na questão da economia digital, vão desde a perda de receita tributária que os Estados não conseguem capturar pela falta de legislação que contemple os novos modelos de negócios, como a questão da (in)justiça fiscal, pois enquanto o comércio tradicional paga a sua justa comparticipação ao Estado, os novos modelos de negócios digitais, que acabam por atrair cada vez mais consumidores, não contribuem para as contas nacionais, criando assim uma discriminação e concorrência desleal.

Mas este não é o entendimento geral. E, tal é a prova, se lermos a discussão do tema entre os países da OCDE, do *Inclusive Framework*, para a nova tributação das plataformas digitais. Parte dos membros da OCDE entendem que a participação dos usuários é um fator único e importante na criação de valor para os negócios digitais, devido à enorme recolha de dados pela intensa monitorização da atividade e do comportamento dos utilizadores. Estes países defendem que os utilizadores contribuem com conteúdo, o que pode ser central para o próprio negócio digital, como para a atração de novos usuários e criação de *network*, tal como também a participação dos mesmos é importante para construir a confiança e a reputação de uma determinada empresa, o que contribui para o crescimento da marca e da rede de usuários. Por outro lado, estão os países que veem a recolha dos dados dos consumidores, a sua participação e os dados gerados pelos mesmos, como uma transação entre estes e o negócio, i.e., enquanto os consumidores oferecem os seus dados, o negócio dá uma compensação financeira ou não financeira (por ex., armazenamento de dados, serviços de e-mail ou entretenimento digital) ao consumidor em troca dos seus dados ou da sua contribuição. Nesta perspetiva, os dados não são diferentes de outros *inputs* de que advêm de outros negócios ou de outros terceiros (por ex., armazenamento de dados, eletricidade). Essencialmente, estes países que vêm a relação do consumidor-negócio como uma transação, com benefício para ambas as partes, defendem que este tipo de serviços deveria estar sujeito a tributação sobre o rendimento, reconhecendo, contudo, sobre essa perspetiva, que este tipo de negócios, onde não há propriamente uma transação financeira, é raramente capturado pelos sistemas fiscais através da tributação do rendimento. Porém, mesmo neste espectro, há países que seguem pelo caminho de que os dados dos consumidores devem ser vistos como ativos intangíveis[97].

Portanto, há várias formas de percecionar de que maneira deve ser feita a tributação dos dados e se esta deve ser feita. E, apesar de já haver um maior consenso entre os vários países quanto à tributação de rendimento gerado

[97] *Supra* nota 29, p.24 a 26.

pelas interfaces e serviços digitais, as questões ainda pairam no ar: devem os dados ser tributados? Se sim, porquê? E como? Ora bem, é exatamente esta problemática que se quer ver debatida neste capítulo.

4.1. NEXO

O primeiro exercício que se tem de fazer antes de qualquer proposta de tributação, como se viu no Cap.II, é estabelecer o nexo.

Recaindo nas situações já existentes no contexto tributário, tenta-se estudar a efetividade de uma adoção das mesmas à economia digital, particularmente, à criação de valor dos dados pessoais.

Ora, neste caminho, duas das tentativas de estabelecer o nexo é a comparação da recolha dos dados dos indivíduos à extração dos recursos naturais, e a simbiose dos dados pessoais à ideia de propriedade intelectual, dando lugar a direitos de autor.

Realisticamente, ambas as situações dão direito a *royalties*. Enquanto propriedade intelectual, os *royalties* dão lugar a pagamentos remuneratórios pela troca do direito de fazer uso da tal propriedade (que pode consubstanciar, por ex., em direitos de autor, patentes, marcas), enquanto para as atividades extrativas, os *royalties* consistem numa compensação pelo direito de extração de um recurso natural[98].

E é sobre estas duas comparações que se se irá debruçar nos subcapítulos seguintes.

a) Como recurso natural

Uma das muitas analogias que se faz então é entre a extração dos dados dos usuários e a extração dos recursos naturais.

Tal como as companhias que exploram os depósitos naturais no solo para a extração de crude, usando tecnologia de extração e exploração, os dados dos usuários são recolhidos dos indivíduos através de serviços digitais "gratuitos". Da mesma forma, as companhias de extração ou vendem o crude às refinarias, ou processam e refinam elas próprias, transformando o crude em produtos à base de petróleo para venda posterior; já os dados são negociados entre corretores ou processados para facilitar o fornecimento de serviços intensivos de dados geradores de receita[99].

Assim, além disso, as empresas extrativas, como empresas comerciais que são, utilizam a riqueza do solo para proveito próprio e para a criação de lucro. Dirigem-se a uma determinada fonte de matérias-primas e exploram-na, extraindo-a do terreno para, posteriormente, a trabalharem e gerarem receita. Com esta atividade, o que acontece de facto é que o solo empobrece,

98 *Supra* nota 1, p.37 a 38.

99 *Supra* nota 1, p.12.

pois o setor extrativo está vocacionado essencialmente para os recursos não renováveis (fala-se aqui do ouro, minérios, crude, entre outros), como a própria expressão indica: há um fim. Logo, posteriormente, não havendo a sua produção ou renovação, o solo esgota-se nos recursos que fornece. E, se esse território está inserido dentro de fronteiras, pertencerá então a uma determinada jurisdição, o que significa que tais recursos pertencem à nação desse Estado onde se encontram as tais reservas.

De forma sucinta, há, então, um levantamento de recursos, que pertencem a um Estado, por parte de uma empresa que os retira para produzir produtos e fornecer serviços com o objetivo de atingir o lucro, ao mesmo tempo que o solo vai empobrecendo e esse Estado, consequentemente, vê escassear os seus recursos.

O mesmo paralelo se pode fazer com a recolha dos dados. Então, tal como há a extração dos recursos também há a extração dos dados. Os dados são propriedade dos seus tutores que se veem extraídos deles por empresas que, depois de os trabalharem e analisarem, vão utilizá-los como um produto final para a venda ou a transmissão, ou como base para melhorar e rentabilizar o negócio, o qual indiretamente acaba por significar mais rendimento para a empresa, pois esta consegue oferecer um serviço ou um produto melhorado e muito mais personalizado.

Tal como os recursos naturais, os dados são factos retirados de uma situação por um terceiro para fins lucrativos sem que haja por isso uma contrapartida direta para os expropriados, o Estado ou os indivíduos.

No caso das indústrias extrativas, seja maquilhada por contribuição, taxa, *royalty*, participação na produção, a verdade é que as compensações, para além do objetivo de obter mais receita, têm exatamente como finalidade obter uma recompensa pela utilização dos recursos nacionais[100]. O objetivo principal dos regimes fiscais para o setor extrativo é essencialmente obter uma compensação pelo empobrecimento do território, pela extração dos materiais que se encontram em tal jurisdição.

Nesta linha, seguindo a lógica aplicada à extração dos recursos naturais, então, o simples facto de uma empresa se apoderar dos dados dos utilizadores, poder-se-ia pensar na aplicação de uma contribuição como recompensa daquele apoderamento.

Vejamos, de todas as figuras de tributos, aquela à qual nos aproximamos com esta explicação é a contribuição. Esta constitui uma prestação pecuniária e coativa exigida por uma entidade pública, em contrapartida de uma prestação administrativa presumivelmente provocada ou aproveitada pelo sujeito passivo. Portanto, na base da relação jurídica tributária, há uma troca entre o sujeito passivo, que se insere no grupo de pessoas sujeitas

[100] Tipicamente, os regimes fiscais combinam instrumentos de tributação baseados na produção e no lucro, o primeiro como compensação e o segundo em sede de rendimento. Os tributos baseados na produção, normalmente, estão em forma de *royalties*. *Supra* nota 1, p.37.

à contribuição, porque se presume que provoquem os mesmos custos ou aproveitem os mesmos benefícios, e a administração[101].

Assim, a contribuição poder-se-ia aplicar às empresas que façam da recolha dos dados dos usuários uma atividade económica, seja a atividade principal ou secundária. Se uma companhia recolhe os dados dos seus utilizadores para, posteriormente, os trabalhar e/ou comercializar, então os governos deveriam poder exigir a tal contrapartida, pela contribuição, pela extração ou acesso aos dados dos usuários no radar da sua jurisdição, como se estes compreendessem um ativo nacional ao qual a empresa se está a fazer valer para retirar benefícios.

Porém, esta analogia entre os recursos naturais e os dados, para o estabelecimento do nexo e posterior aplicação de uma contribuição, não é nítida. Enquanto nos recursos não renováveis é a sua escassez que gera rendas económicas elevadas, quando extraídos; no caso dos dados pessoais, a renda, se aplicável, não é devida à escassez do recurso, mas, sim, é devida às características naturais do monopólio e exclusividade dos negócios que os detêm[102].

Daí que segundo a visão de Robert Goulder, havendo a associação entre o acesso aos dados pessoais e a extração de recursos naturais, devido à não escassez do primeiro pela extração, a comparação deve ser feita com os recursos renováveis, como a energia solar e eólica, e não com os primeiros. O que, na perspetiva do autor, até resolve a opção de aplicação de uma contribuição[103].

Faça-se o raciocínio: se a contribuição, no seu cerne, tem como objetivo primordial compensar o país pela perda ou desgaste de um bem pertencente ao Estado, provocando custos para este, então a contribuição não poderia ser aplicada aos dados pessoais, visto que estes não escasseiam pelo simples facto de serem extraídos, ou seja, não há uma perda, pois os dados são um recurso *ad eterno*, ao contrário dos recursos não renováveis. Sem margem para dúvida, neste seguimento, concordamos com a perspetiva do autor de que a figura da contribuição não é a mais apropriada.

Mas, pelo que foi explicado anteriormente, a contribuição também se aplica quando um determinado grupo de indivíduos presumivelmente beneficia do Estado. Ora, se a apropriação dos dados dos usuários não esgota o recurso, por não haver um desgaste ou custos para o Estado, pelo menos cria benefícios para o sujeito passivo. E, para a sua aplicação, não é necessário, na perspetiva de Sérgio Vasques, que haja um benefício ou um custo efetivo, basta-se com a mera previsibilidade. Ora, os dados dos usuários quando recolhidos em bruto não têm qualquer valor para a empresa, só pelo seu tratamento e análise é que o vão adquirir. Contudo, há, ao que chamamos, uma presunção de comercialidade, i.e., no momento da recolha dos dados estes são possíveis vetores de

---

101 Sérgio Vasques, *Manual de Direito Fiscal*, Coimbra, Edições Almedina, S.A., 2015. P.260 a 264.

102 *Supra* nota 1, p.12.

103 Robert Goulder, *Should Data Extraction Be Taxed as a Natural Resource?*.

valor para a empresa, caso não o fossem, não haveria todo o investimento em *hardware* e *software* por parte da empresa para a extração de tais dados: se o faz é porque os dados que vai extrair são potencialmente valiosos.

Deste modo, pode-se afirmar que a aplicação de uma contribuição continua a fazer sentido. No entanto, se olharmos para o art.4º, nº3 LGT, este refere que os benefícios arrecadados pelo sujeito passivo têm de ser "*em resultado de obras públicas ou da criação ou ampliação de serviços públicos*". Portanto, é também pressuposto que haja uma intervenção do Estado, por via da administração, que indiretamente gera benefícios para o sujeito passivo. Bem, no caso da recolha dos dados, não há uma intervenção do Estado, há, sim, uma ação por parte dos utilizadores que disponibilizam ou geram dados, os quais as empresas, através do seu investimento em tecnologias e *know-how,* recolhem e geram valor a partir dos mesmos. Assim, o exercício da aplicação de uma contribuição fica difícil. Exceto, se considerarmos a perceção do legislador tributário português de que "*as contribuições especiais* (…) *são consideradas impostos*", como aquele artigo menciona, e aí a tal quase bilateralidade entre o custo/benefício e a ação administração estatal, tal como a exigência de um benefício certo ("*pois é presumível*"), parece não ser mais exigida visto que os impostos são tributos caracterizados pela sua unilateralidade[104]. Só com um pensamento similar será possível, a meu ver, aplicar uma contribuição.

Assim, de facto, o paralelo com os recursos naturais traz perceções interessantes para um tratamento fiscal dos dados, particularmente quando se quer estabelecer o nexo e alocar novos direitos tributários. Contudo, tal pertinência perde força aquando da discussão sobre o tipo de tributo a aplicar.

No caso de se pensar em tributar a recolha dos dados só pelo simples facto de estes serem extraídos, então, o tributo mais apropriado será a contribuição especial, numa visão de que os usuários são expropriados dos seus dados, esses que vão, em princípio, criar valor para a empresa que os recolheu e, por obrigação solidária, deveria então compensá-los por meio de pagamento de um tributo.

E, havendo a sua aplicação pela tributação *per se* dos dados, então o evento tributável, a ser considerado, será apenas e somente o momento da extração dos dados, ou seja, quando a empresa tem acesso a estes, mesmo antes de qualquer ação sobre eles[105]. Assim, só pelo facto de as empresas recolherem os dados dos usuários isso já é razão suficiente para que o Estado da jurisdição dos usuários tribute a empresa, não interessando o que a empresa faz posteriormente com os dados e se, efetivamente, retira valor dos mesmos.

---

104 A simbiose entre a figura das contribuições e os impostos não é novidade. Até há pouco era entendimento geral da jurisprudência constitucional portuguesa de que as contribuições deveriam ser tratadas como impostos, por lhes faltar a bilateralidade rigorosa das taxas e porque também para a sua criação há a exigência constitucional da reserva de lei parlamentar (Acórdãos nº277786, de 8.10.1986; nº313/92, de 6.10.1992; nº410/2000, de 3.10.2000; e, nº616/2003, de 16.12.2003. *Supra* nota 101, pág-281 a 283.

105 *Supra* nota 8.

b) Como obra intelectual

Se anteriormente se quis aproximar a extração dos dados dos usuários à extração de recursos naturais, agora o paralelismo é feito com a propriedade intelectual.

Nesta nova visão vê-se os dados dos indivíduos possíveis geradores de direitos de autor, onde cada indivíduo é o autor e proprietário dos seus próprios dados e que os pode dispor caso um terceiro intente utilizá-los para outros fins, nomeadamente, comerciais.

Se no passado, o acesso às ideias era por intermediação da imprensa (quiosques, livrarias, bibliotecas, televisão, rádio e até discursos públicos), atualmente o acesso às ideias passa maioritariamente para o digital, pelo uso dos computadores, *Tablets* e telemóveis para o acesso a motores de busca, *websites*, redes sociais, para enviar textos, correios eletrónicos e mensagens instantâneas[106].

O que leva Neil Richards a constatar que qualquer tecnologia que utilizámos no seguimento do nosso pensamento implica a nossa, ao que ele chama, "*intelectual privacy*" (privacidade intelectual, traduzido)[107]. Na sua perspetiva, quando utilizámos motores de busca para aprender algo, responder a questões e dúvidas, como um auxílio ao nosso pensamento, então, o simples ato de pesquisar será, efetivamente, uma forma de pensamento[108]. É através da nossa procura pelo conhecimento que construímos os nossos ideais, as nossas convicções e formas de pensamento. Tal conhecimento retirámos de várias fontes, seja por meio dos livros, artigos no jornal, debates, notícias, entre outros. Contudo, estas fontes têm migrado para o meio digital e atualmente buscamos os mesmos recursos no meio digital, através da colocação de perguntas, dúvidas e questões no motor de busca (como a Google), ou lemos um livro eletrónico (por ex., no Kindle ou através da Amazon), e acedemos a notícias online que mais nos interessam, tudo para construirmos o nosso pensamento.

A única diferença entre os tempos anteriores à era da digitalização e os tempos modernos é a monitorização das nossas atividades no meio virtual. As plataformas digitais conseguem, através das nossas pesquisas, da criação de conteúdo online e das nossas conexões sociais, traçar o nosso perfil, os nossos interesses, tendências, crenças e opiniões. Portanto, ter acesso ao nosso pensamento. O que leva Richards a afirmar que então há uma privacidade intelectual que tem de ser salvaguardada.

Por isso, se queremos preservar a nossa liberdade de pensamento, sem que exista uma espionagem, monitorização e interferência, então deverí-

---

106 Neil Richards, *Intellectual Privacy – Rethinking Civil Liberties in the Digital Age*, Nova Iorque, OXFORD University Press, 2015. P. 97.

107 *Supra* nota 106, p. 122.

108 *Supra* nota 106, p.122.

mos abarcar estas tecnologias num conceito de privacidade intelectual[109]. A privacidade intelectual deveria, então, não ser apenas estendida às livrarias, como deveria incluir qualquer dado que revelasse os pensamentos e devaneios de uma mente humana[110].

Essencialmente, aquilo que Richards advoga é a combinação entre uma regulamentação da privacidade mais vocacionada para as novas tecnologias, e uma regulamentação da liberdade de expressão. Enquanto a primeira pretende restringir a coleção e o fluxo de informação, a segunda permite-o[111].

Esta privacidade intelectual de que se falou é construída por dados: pessoais e não pessoais. Isto, porque os dados pessoais (assim como a morada, o nome, a idade, os dados de saúde, o número de identificação fiscal, o número de utente, entre outros), como tal, são aqueles que identificam uma determinada pessoa; mas os dados não pessoais (aqueles que são gerados pelo usuário, da mesma forma que os "gostos" em publicações, a partilha de mensagens e chamadas, as conexões de amizades, o tempo que se passa em determinada página, entre outros) que, individualmente não são identificativos de uma pessoa, mas que, em combinação, conseguem identificar o indivíduo, traçando todo o seu quotidiano, personalidade, convicções, e consequentemente o seu pensamento, devem ser considerados também eles dados pessoais[112]. Assim, como foi até aqui, quando nos referimos a dados pessoais, incluímos também os dados gerados pelo usuário.

A pergunta que cabe colocar agora é: podem então os dados pessoais e não pessoais serem considerados direitos de autor?

Efetivamente, a regulamentação da proteção dos dados pessoais abriu a porta para a comparação com os direitos de autor, principalmente no seio da UE. Focando-nos no Regulamento Geral sobre a Proteção de Dados (RGPD)[113], este passou a conceder, entre outros, os seguintes direitos ao autor dos dados: o direito de retificação (art.16º), o direito a ser esquecido (art.17º), o direito da portabilidade dos dados (art.20º) e o direito de oposição (art.21º). Deste elenco pode-se retirar uma certeza e um paralelismo. A certeza de que o titular dos dados pessoais passa a ser visto como o proprietário dos seus dados e, desse modo, a similaridade com os direitos pessoais de autor é inegável.

---

109 *Supra* nota 106, p.122.

110 *Supra* nota 106, p.161.

111 *Supra* nota 106, p.154.

112 Mor Bakhoum, Beatriz Gallego, Mark-Oliver Mackenrodt, Gintare Surblyte-Namaviciene, *Personal Data in Competition, Consumer Protection and Intelellectual Propoerty Law – Towards a Holistic approach?.* P.199

113 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Diploma disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679

Vejamos, os direitos de autor são em si direitos que incidem sobre obras intelectuais, literárias e artísticas[114], por meio da criação humana[115].

Se se seguir a doutrina filosófica de Kant[116], o direito de autor deve ser entendido como uma manifestação particular da tutela da personalidade do autor. Nesse entendimento, correspondendo o pensamento a uma manifestação da personalidade de uma pessoa, o direito de autor deverá ser entendido como um direito de personalidade[117], que protege as obras do espírito como componentes da esfera pessoal de uma pessoa. E, portanto, a atividade prévia da criação intelectual, sendo uma componente essencial da

[114] Segundo a letra do artigo 2ºbis, nº1 da Convenção de Berna, entende-se por obras literárias e artísticas qualquer obra no campo literário, científico e artístico, qualquer que seja o modo ou forma pela qual se expressa, como livros panfletos e outros tipos de escrita; palestras, discursos, sermões e outros da mesma natureza; obras dramáticas ou dramático-musicais; trabalhos coreográficos em espetáculos de linguagem gestual; composições musicais com ou sem palavras; obras cinematográficas às quais são assimiladas obras expressas por um processo análogo à cinematografia; trabalhos de desenho, pintura, arquitetura, escultura, gravura e litografia; obras fotográficas às quais são assimiladas obras expressas por um processo análogo à fotografia; funciona de arte aplicada; ilustrações, mapas, plantas, esboços, e trabalhos tridimensionais geográficos, topografia, arquitetura ou ciência. Ver *website* WIPO: https://wipolex.wipo.int/en/text/283693. No âmbito da UE, no que diz respeito aos direitos de autor, importa também referir a Diretiva 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de Maio de 2001, relativa à harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação. Diploma disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001L0029

[115] Luís Manuel Teles De Menezes Leitão, *Direitos de Autor*, Coimbra, Edições Almedina S.A., 2011. P.69.

[116] A influência de tal escola de pensamento, em considerar que a qualificação do direito de autor deve corresponder a um direito de personalidade, encontra mérito nos direitos pessoais de autor: o direito ao inédito, o direito de retirada, o direito à menção do nome na obra, direito de reivindicar a paternidade da obra, o direito de assegurar a genuinidade e integridade da obra, o direito de efetuar modificações na obra e o direito de acesso à obra. *Supra* nota 115, p.40 a 41 e 147 a 158.

[117] Os direitos de personalidade são direitos inatos e subjetivos que incidem sobre a esfera pessoal do indivíduo, e pertencem à pessoa como manifestações da personalidade. Daí que, o bem jurídico protegido é o próprio ser da pessoa. No Código Civil Português (CC), o regime dos direitos de personalidade está explanado entre os arts.70º e 81º. Do elenco de direitos fazem parte: o direito ao nome e pseudónimo (arts.72º a 74º CC), o direito à confidencialidade (arts.75º a 78º CC), o direito à imagem (art.79º CC), o direito à reserva sobre a intimidade da vida privada (art.80º CC), o direito à vida, o direito de não ser privado da vida contra a vontade, à liberdade e integridade de consciência, à integridade física e psíquica, à liberdade, à honra, à imagem social e de caráter, à saúde e ao repouso, à autodeterminação quanto aos dados pessoais no contexto da informática, à proteção contra a manipulação genética e, por fim, ainda, a uma morte digna (todos estes incluído no direito geral de personalidade presente no nº1 do art.70º CC). Heinrich Hoster*, A parte geral do Código Civil Português – Teoria Geral do Direito Civil*, 6º Reimpressão, Coimbra, Edições Almedina S.A., 2012. P.259 a 260 e p.304 a 305.

natureza humana, tem de ser vista sempre como uma emanação da personalidade do seu titular[118].

Deste modo, se o pensamento é imprescindível para a criação intelectual e esta resulta e depende exclusivamente daquele (do intelecto), então poder-se-ia concretizar dizendo que: a obra intelectual[119] será então o dado pessoal (e o gerado) *per se* que, através da intervenção humana (pelo uso das plataformas digitais e dos aparelhos eletrónicos), exterioriza a personalidade e o pensamento do autor (por tudo o que foi acima explicado).

No entanto, esta afirmação está longe de ser consensual. E, respondendo à pergunta acima colocada, não afirmarei que os dados pessoais possam dar direito a um direito de autor *sui generis*: no máximo, a ele é comparável. Não se querendo fazer incidir muito no direito de autor, pode-se seguir a doutrina internacional sobre a discussão, não se os dados pessoais devem ser alvo de proteção via direitos de autor, mas sim, se devem ser protegidos como um direito de propriedade intelectual, no geral[120][121].

Sendo os dados pessoais comparáveis aos direitos de autor, especificamente, ou à propriedade intelectual, em qualquer um dos casos, para lá dos direitos pessoais no escopo jurídico do direito, há também os direitos patrimoniais, onde entra o *royalty*. Os *royalties* são remunerações pagas pelo direito de uso de uma propriedade intelectual.

Nesta linha, o Fundo Monetário Internacional (FMI) propõe que se desenhe uma espécie de *royalty*[122] para os dados pessoais.

Na visão de Aqib e Alpa, a base do *royalty* pode ser sobre o valor do fluxo de dados recolhidos de um determinado país por uma companhia que pretende fazer uso dos mesmos. Alternativamente, se a empresa detém a

---

118 *Supra* nota 115, p.40 a 41.

119 Nos direitos de autor, entende-se por obra intelectual exteriorizada, qualquer obra que resulte, primeiramente, da criação humana, que, em seguida, acrescente algo de novo e ainda seja exteriorizada, i.e., que não permaneça no foro íntimo do autor sendo revelada aos outros de forma apreensível pelos sentidos. *Supra* nota 115, p.69 a 71.

120 A propriedade intelectual, como a própria expressão indica, compreende aquilo que vem do intelecto, e é dividida em dois tipos de categorias, o direito de autor e direitos conexos, e a propriedade industrial. Enquanto os primeiros abrangem as obras literárias, artísticas e científicas, o segundo cobre as patentes de invenção, os desenhos ou modelos, as marcas, modelos de utilidade, logótipos e denominações de origem e indicações geográficas. Documento disponível em: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_450_2020.pdf. *Cfr. Supra* nota 115, p.13 a 15.

121 Discussão diferente é se os dados pessoais devem cair na alçada dos direitos reais, e, portanto, alvo de direitos de propriedade em geral, ou no direito especial de propriedade intelectual. Leon Trakman, Roberts Walters, Bruno Zeller, *Is Privacy and Personal Data Set to Become the New Intellectual Property?* (Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3448959>).

122 De referir que a proposta do FMI foi desenhada em comparação com os *royalties* aplicados às atividades extrativas. No entanto, pareceu-nos mais apropriada aplicar a ideia do *royalty* à comparação com os direitos de autor.

propriedade sobre os dados, ao invés de apenas ter acesso aos mesmos, o que se pode imaginar é a aplicação do *royalty* sobre o armazenamento dos dados num dado período, argumentando-se que, como estão sempre ao dispor do seu proprietário (i.e., a empresa), há um uso e uma criação de valor a partir dos mesmos dados repetidamente[123].

Caso seja difícil determinar os métodos a serem utilizados para a aplicação das anteriores propostas, pode-se considerar outro meio. Esta terceira via referida no relatório inclui dois níveis. O primeiro seria calcular o montante dos rendimentos dos serviços digitais de uma companhia que foram gerados pelos usuários de um determinado país. Ou seja, olha-se para os rendimentos que são criados numa certa jurisdição. Quando se estipule o *quantum* gerado, o segundo será a aplicação de uma subtração (estandardizada) nesses rendimentos, de forma que seja contabilizado o valor acrescentado pelo processamento e tratamento dos dados[124].

Alguns problemas são levantados. Um deles é o facto de os dados não serem bens físicos, pelo que o mesmo conjunto de dados pode ser combinado, processado e usado simultaneamente na produção de vários bens e serviços, o que dificulta a aplicação das fórmulas para determinação do seu valor. Outro apontamento feito é de que tem de existir uma coordenação entre os países, sob pena de serem aplicadas simultaneamente e de forma inconsistente várias fórmulas de pagamento pelo valor dos dados[125].

Apesar de o FMI referir-se ao *royalty* como um instrumento fiscal, aqui as considerações são feitas tendo como entendimento que o r*oyalty* é um pagamento pelo direito de se fazer uso da propriedade intelectual e, que, por isso, é regulado por direito especial que se insere no ramo do direito privado, não havendo ligações ao direito fiscal.

Nessa linha, se os usuários têm propriedade sobre os seus dados então há lugar a um direito a remuneração[126], pelo que as multinacionais teriam de proceder ao seu pagamento para estarem autorizadas a utilizar os dados dos usuários. Como se configura logisticamente impraticável o pagamento a bilhões de usuários, poderia entrar o Estado como intermediário do coletivo, ou seja, intervir na estipulação de uma remuneração às multinacionais não como o proprietário dos dados, mas como representante desses proprietários[127].

Na visão de entender que os dados poderiam dar lugar a direitos de autor, aplicando-se-lhe um *royalty*, o FMI adverte que se essas remunerações forem tidas como um substituto ao IRC, ao invés de ser um complemento, e não haver uma creditação em sede do Imposto sobre o Rendimento de

123 *Supra* nota 1, pp. 37a 41.

124 *Supra* nota 1, pp. 37 a 41.

125 *Supra* nota 1, p. 39.

126 Remunerações que entrariam posteriormente para os rendimentos da categoria B na declaração de IRS dos indivíduos para serem, então, alvo de tributação em sede de IRS (veja-se os artigos 3º, nº1, c) e 3º, nº5 CIRS).

127 *Supra* nota 1, p. 23.

Pessoas Coletivas (IRC) a pagar na jurisdição da residência, então o risco de não haver um consenso multilateral e com isso nascer uma dupla tributação, é enorme. Ainda, se as medidas foram aplicadas unilateralmente pode haver lugar a retaliação. Na visão dos autores Aqib e Alpa, na aplicação do *royalty,* os países, sejam os desenvolvidos ou os em desenvolvimento, devem considerar um valor modesto paralelamente ao IRC, com um adicional mecanismo de captura para projetos particularmente rentáveis[128].

4.2. ESCOPO

Estabelecido o nexo, a determinação do escopo será de trabalho mais fácil.

Em ambas as visões pretende-se então tributar os dados. Se na primeira se faz a comparação com a extração dos recursos naturais para a aplicação de uma contribuição, na segunda atribui-se aos usuários a propriedade dos seus dados que o legitima, por isso, a cobrar um género de *royalty*.

Ora, na primeira visão o foco é a recolha dos dados. O *ratio* é de que só pelo simples facto de que há uma extração dos dados pessoais, deve haver uma compensação realizada através do pagamento de uma contribuição. Portanto, não importa os momentos posteriores à recolha dos dados, o único a ser considerado é o primeiro. Se o que realmente interessa é o momento da recolha dos dados, então, o tipo de dados em causa, serão os dados em bruto (i.e., sem ainda ter havido um tratamento nem armazenamento), não interessando se são dados pessoais ou dados gerados pelos utilizadores.

Na segunda visão, o que está em causa é o direito de fazer uso dos dados dos utilizadores como se aqueles fossem os seus proprietários. Neste contexto, o evento tributável será quando o direito de propriedade (intelectual) passa da esfera jurídica do utilizador para o operador económico. Portanto, o momento tributável será quando a entidade detém o direito. Para tal, não importará fazer a distinção entre o tipo de dados, pois considera-se que os dados gerados pelos utilizadores serão também eles tidos como dados pessoais.

Em suma, apesar de se procurar por uma compensação, o *ratio* por detrás das duas visões é diferente. Numa é pelo simples facto de haver uma extração, na outra é pela aquisição de um direito.

5. CONSIDERAÇÕES FINAIS

Após a análise das várias formas de tributar os dados dos usuários, seja de forma indireta, pelo Pillar One da OCDE, pelas soluções encontradas pelos países, seja de forma direta, pela sugestão das duas novas perspetivas, cabe agora fazer algumas considerações.

---

128 *Supra* nota 1, pp. 37 a 41.

A primeira, e que é de alta importância reter, é de que o objeto, tanto da proposta da OCDE, como dos vários países, engloba os rendimentos provenientes dos serviços ou bens prestados, em sede de IRC, o que por si só não implica o afastamento da aplicação de uma das visões propostas.

O foco deve estar se se pretende tributar os rendimentos das empresas presentes na economia digital, ou se se quer tributar os dados *per se*. Tanto para uma como para a outra tem de existir um nexo e um escopo. Mas uma não se confunde com a outra, pois se a tributação for *a posteriori*, nos rendimentos, é sobre esses, e somente sobre esses, que vai incidir a tributação, enquanto se for *a priori* pelo simples facto de se entender que os dados devem ser tributados por si só, então estamos a falar de um objeto tributável diferente.

Desse modo, este trabalho não esgota a sua pertinência no momento em que haja um acordo internacional ao nível da OCDE. Porque mesmo existindo, ainda há a possibilidade de aplicação de uma tributação sobre os dados pessoais baseada numa das duas perspetivas estudadas, por se focarem em momentos e factos diferentes dos da OCDE.

Começando pelas considerações sobre o segundo capítulo.

Na impaciência de esperar por um acordo global para a tributação das multinacionais e com o risco de nem sequer chegar a existir tal acordo, os países no presente trabalho decidiram então começar a implementar medidas para conseguir capturar a receita desses grupos. No entanto, a maioria das medidas implementadas são temporárias, sendo mesmo referido nos diplomas legislativos de que a tributação vigora até haver um acordo multilateral, fazendo-se menção à proposta da OCDE que incluirá os dois pilares. Factor pelo qual, a maioria das soluções apresentadas pelos países, muitas delas, já em vigor, são um espelho da proposta da OCDE.

A aplicação da tributação desenhada pela OCDE trará maior justiça fiscal entre as empresas. I.e., colocará as empresas num mesmo pé de igualdade. Pela tributação dos negócios digitais, as multinacionais vão passar a pagar impostos sobre o seu rendimento de igual forma que as empresas com as quais fazem concorrência (in)direta[129].

Mas, se por um lado traz maior igualdade perante a Lei, por outro diminui a competitividade fiscal entre Estados. Tendo em consideração o Pillar Two, que implementa uma taxa de imposto mínima global de 15%, isto significará que os Estados perderão (outra) parte da sua soberania fiscal (uma parte muito importante, principalmente, para os países da Zona Euro que já viram a sua soberania diminuída aquando da cedência da gestão da moeda ao Banco Central Europeu) na determinação da taxa de imposto a aplicar. É verdade que tal proposta e tal combate ao abuso fiscal só será possível

[129] Pense-se no exemplo de uma livraria de rua que está sujeita às obrigações fiscais, nomeadamente, o IRC, enquanto a Amazon, uma plataforma digital que vende livros, como até há pouco não era abrangida pela legislação tributária e, consequentemente, não pagava impostos sobre o rendimento nas jurisdições em que vendia os seus produtos.

com uma ação global concertada para desincentivar as empresas a usarem outros sistemas fiscais menos gravosos.

A meu ver, para as medidas contidas no Pillar One e Pillar Two, que têm como objetivo combater as práticas BEPS, serem efetivas tem de se verificar: primeiro, uma adesão geral dos Estados parte do *Inclusive Framework* da OCDE, pois se as jurisdições que normalmente são atrativos fiscais para as multinacionais não forem parte no acordo multilateral, a eficácia de tal proposta ficará aquém do esperado (apesar de mesmo assim conseguir ainda aplicar-se eficientemente até porque os países normalmente apontados como sendo uma atração por terem sistemas fiscais mais favoráveis, como o caso da Irlanda e Países Baixos, por onde passa a maioria do planeamento agressivo das multinacionais, vão integrar este acordo), e, segundo, sabendo de antemão que os paraísos fiscais vão continuar a existir, então é necessário que paralelamente haja mecanismos eficazes de transparência à escala global entre os vários Estados.

Passando agora às considerações sobre todas as propostas de tributação direta ou indireta dos dados pessoais, incluindo, por isso, a proposta da OCDE, dos países, e as duas novas perspetivas.

Há possíveis pontos positivos a salientar com a entrada em vigor de tais propostas.

Seja para os países em desenvolvimento, seja para os países desenvolvidos, os ganhos são transversais a todos. Sem dúvida que, com a nova tributação, os países vão conseguir capturar situações tributáveis que antes não conseguiam, pelas lacunas presentes na legislação tributária; portanto, vão conseguir, assim, captar mais receita para as suas contas.

Contudo, há que ter em conta o surgimento de uma repercussão fiscal[130]. Com a entrada em vigor de qualquer uma das propostas apresentadas nos dois capítulos acima (Cap.II e Cap.III) os custos, sejam de *compliance,* sejam pelo pagamento dos novos impostos e tributos, irão inevitavelmente diminuir os lucros das multinacionais. E, como estas não pretendem suportar o custo, a solução que normalmente encontram é aumentar o preço final do serviço prestado ou do produto.

Claro está que a repercussão fiscal só terá lugar quando a elasticidade da procura for rígida, pois o vendedor sabe que o comprador é pouco sensível ao aumento do preço[131]. Mas, mesmo dependendo da elasticidade da procura, convém ter sempre em conta a possibilidade de haver uma repercussão para os utilizadores. Seria irónico que o consumidor final acarretasse com

---

[130] A repercussão fiscal consiste na transferência do peso económico de um tributo para pessoa diferente do sujeito passivo através da respetiva integração desse no preço de um qualquer bem ou serviço que o sujeito passivo vai pagar. A forma mais comum é a chamada repercussão descendente, que tem lugar quando o vendedor soma o tributo ao preço de um bem, fazendo com que o comprador o suporte. *Supra* nota 101, pp. 397 a 400.

[131] *Supra* nota 101, pp. 397 a 400.

tais custos, quando as propostas de tributação de dados, sejam elas quais forem, vêm em sentido de auxiliar os Estados a arrecadar mais receita para as suas despesas e ofícios nacionais.

Outra consequência é o fim dos serviços gratuitos, passando as empresas a implementar *"pay-for-privacy model"* onde dão a opção ao utilizador de manter os seus dados estritamente confidenciais, por exemplo, por um período de 12 meses, na troca de um pagamento anual de privacidade[132].

Por fim, todos os modelos de possíveis tributações vão obrigar a que haja uma enorme adaptação das autoridades tributárias às novas regras, como exigir um maior investimento em mecanismos e ferramentas tecnológicas para acompanhar a adaptação do Direito Fiscal à economia digital, sob pena de não se conseguir implementar eficazmente as soluções encontradas.

Serei particularmente a favor de qualquer solução estudada nesta investigação, desde que se assegure firmemente o princípio da neutralidade[133]. Que nos seus termos, o Estado pode estar legitimado a tributar para ter mais uma fonte de receita para fazer face às despesas nacionais, mas nunca deve, para isso, onerar em demasia os operadores económicos e os contribuintes ao ponto de mudar o seu comportamento e hábitos de consumo. Tal situação só resultaria em disrupções económicas, travando o investimento e o desenvolvimento económico de um mercado.

Outros problemas poderiam ser aqui levantados. Sem dúvida que este tema é bastante complexo e não só levanta várias questões secundárias, como questões muito técnicas. Daí que os legisladores tributários têm tido bastantes dificuldades em adaptar os seus sistemas à economia digital.

Não se tendo entrado demasiado por temas secundários, espera-se que este trabalho seja oportuno na demonstração das tendências que se fazem sentir no contexto internacional para a tributação da economia digital, mais concretamente, dos dados pessoais.

Para além do estudo do Pillar One, e dos vários países, ambicionaram-se duas formas de possível tributação dos dados pessoais. Estas duas visões apresentadas não configuram propostas, mas sim apenas ideias através das quais seja possível estabelecer um nexo e, consequentemente, desenhar um novo tributo. Sabendo que são polémicas e que dão azo a várias opiniões, o objetivo das duas perspetivas foi de criar discussão sobre o tema para um futuro em que haja uma vontade de tributar os dados e não só os rendimentos das multinacionais.

---

132 *Supra* nota 103.

133 Segundo o princípio da neutralidade, "o imposto ideal será aquele que retira do contribuinte em proporção da sua riqueza ou despesa, de modo que altere o mínimo o seu padrão de comportamento". Glória Teixeira, *Manual de Direito Fiscal*, 5º Edição, Coimbra, Edições Almedina S.A., 2019. PP. 51 a 52.

Por tudo o que foi dito, penso que este trabalho atingiu o objetivo principal, enunciado na introdução, que era o de demonstrar as várias opções através das quais o mercado de dados pode ser tributado.

De notar que, em ambos, tanto na solução da OCDE, tal como nas propostas apresentadas pelos países, há ainda pontos sob discussão e análise, por isso, alerta-se o leitor que para o desenvolvimento das situações anteriormente abordadas, foram tidos em conta os dados disponíveis até ao final da escrita deste trabalho, final de junho de 2022, pelo que, aquilo que se disse tem caráter provisório, sob pena de haver mudanças posteriores à publicação deste trabalho.

6. BIBLIOGRAFIA

LIVROS

Enciclopédia Pedagógica Universal, *História da Ciência e da Tecnologia IV e V*, Vol.24 e 25, Portugal, Hiperlivro, ASA ed., 2001.

Enciclopédia Pedagógica Universal, *O Mundo dos Computadores*, Vol. 19. Portugal, Hiperlivro, ASA ed., 2001.

Hoster, Heinrich, *A parte geral do Código Civil Português – Teoria Geral do Direito Civil*, 6º Reimpressão, Coimbra, Edições Almedina S.A., 2012.

Leitão, Luís Manuel Teles De Menezes, *Direitos de Autor*, Coimbra, Edições Almedina S.A., 2011.

Richards, Neil, *Intellectual Privacy – Rethinking Civil Liberties in the Digital Age*, Nova Iorque, OXFORD University Press, 2015.

Teixeira, Glória, *Manual de Direito Fiscal*, 5º Edição, Coimbra, Edições Almedina S.A., 2019.

Vasques, Sérgio*, Manual de Direito Fiscal*, Coimbra, Edições Almedina, S.A., 2015.

CONSULTAS ELETRÓNICAS

Á. De La Cueva González-Cotera & A. Arroyo Ataz, Spain - Corporate Taxation, *in Country Tax Guides IBFD*, disponível em https://research.ibfd.org/#/doc?url=/document/cta_es_s_14 (12.05.2022)

Adda, M, Lorenzi, U, Scandone, F.S., "The new taxing right under Pillar One: preliminary thoughts on potential implications for MNEs", *in International Transfer Pricing Journal*, 2021, disponível em http://link.library.ibfd.org/portal/The-new-taxing-right-under-Pillar-One-/rWZJznc7anE/

Aslam, Aqib, Shah, Alpa, "Tec(h)tonic Shifts: Taxing the Digital Economy", *in IMF Working Paper*, Vol. WP/20/76, 2020, disponível em https://www.imf.org/en/Publications/WP/Issues/2020/05/29/Tec-h-tonic-Shifts-Taxing-the-Digital-Economy-49363

Bakhoum, Mor, Gallego, Beatriz, Mackenrodt, Mark-Oliver, Surblyte-Namaviciene, Gintare, "Personal Data in Competition, Consumer Protection and Intelellectual Propoerty Law – Towards a Holistic approach?", *in Springer*, 2018, disponível em https://books.google.pt/books?id=BQN2DwAAQBAJ&p-g=PA199&dq=personal+data+is+copyright&hl=pt-PT&sa=X&ved=2ahUKEw-j5oPigyof5AhWPgVwKHYt5DHUQ6AF6BAgKEAI#v=onepage&q&f=true

C. (Cesare) Silvani, Italy - Corporate Taxation, *in Country Tax Guides IBFD*, disponível em https://research.ibfd.org/#/doc?url=/document/cta_it_s_14 (12.05.2022)

Dam, H. Van, Kiès, C., Klethi, P-A., Kroon, S. Van Der, Kunen, J-W., Silva, B. Farinha Aniceto Da, "International - Taxing the Digitalized Economy: Key Takeaways from the OECD Public Consultation on the Pillar One and Pillar Two Blueprints", *in International Transfer Pricing Journal*, Vol 28, n.º3, 2021, disponível em http://link.library.ibfd.org/portal/Taxing-the-digitalized-economy--key-takeaways/pggKAvqKXhk/

Deglaire, Emmanuelle, "Taxation of data: the next step?", *in Taxation*, 2019, disponível em http://link.library.ibfd.org/portal/Taxation-of-data--the-next-step/yWWexBFP7f0/

Diretiva 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de Maio de 2001, disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001L0029

G. ErdőS, Hungary - Corporate Taxation, *in Country Tax Guides IBFD*, disponível em https://research.ibfd.org/#/doc?url=/document/cta_hu_s_14. (12.05.2022)

GadžO, Stjepan, "Chapter 2: Legal Fundamentals of Income Tax Jurisdiction in Nexus Requirements for Taxation of Non-Residents' Business Income – A Normative Evaluation in the Context of the Global Economy", *in Books IBFD*, 2018, disponível em https://www.ibfd.org/shop/book/nexus-requirements-taxation-non-residents-business-income-normative-evaluation-context (21.07.2022).

Goulder, Robert, "Should Data Extraction Be Taxed as a Natural Resource?", *in Tax Notes International*, n.º 2020-27839, 2020

https://research.ibfd.org/#/doc?url=/document/dtm_fr (12.05.2022)

IBFD, Austria - Digital Taxation Monitor, disponível em https://research.ibfd.org/#/doc?url=/linkresolver/static/dtm_at (12.05.2022)

IBFD, Brazil - Digital Taxation Monitor, disponível em https://research.ibfd.org/#/doc?url=/document/dtm_br (12.05.2022)

IBFD, European Union - Digital Taxation Monitor, disponível em https://research.ibfd.org/#/doc?url=/document/dtm_e2 (12.05.2022)

IBFD, France - Digital Taxation Monitor, disponível em

IBFD, Hungary - Digital Taxation Monitor, disponível em https://research.ibfd.org/#/doc?url=/document/dtm_hu (12.05.2022)

IBFD, India - Digital Taxation Monitor, disponível em https://research.ibfd.org/#/doc?url=/document/dtm_in (12.05.2022)

IBFD, Indonesia - Digital Taxation Monitor, disponível em https://research.ibfd.org/#/doc?url=/document/dtm_id (12.05.2022)

IBFD, Italy - Digital Taxation Monitor, disponível em https://research.ibfd.org/#/doc?url=/document/dtm_it (12.05.2022)

IBFD, Kenya - Digital Taxation Monitor, disponível em https://research.ibfd.org/#/doc?url=/document/dtm_ke (12.05.2022)

IBFD, Spain - Digital Taxation Monitor, disponível em https://research.ibfd.org/#/doc?url=/document/dtm_es (12.05.2022)

IBFD, Turkey- Digital Taxation Monitor, disponível em https://research.ibfd.org/#/doc?url=/document/dtm_tr (12.05.2022)

IBFD, United Kingdom - Digital Taxation Monitor, disponível em https://research.ibfd.org/#/doc?url=/document/dtm_uk (12.05.2022)

IBFD, United States - Digital Taxation Monitor, disponível em https://research.ibfd.org/#/doc?url=/document/dtm_us (12.05.2022)

Legislação Austríaca, disponível em https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010780

Legislação brasileira, disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2258196, https://www25.senado.leg.br/web/atividade/materias/-/materia/142074, https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2260638

Legislação britânica, disponível em https://www.legislation.gov.uk/ukpga/2020/14/part/2/enacted, https://www.gov.uk/hmrc-internal-manuals/digital-services-tax, https://www.legislation.gov.uk/ukpga/2020/14/schedule/8/enacted

Legislação do acordo *Unilateral Measures Compromise*, disponível em https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=5EEE687F-D512-475B-B940-F85237E00E1C&filename=1575%20-%20Joint%20Statement%20on%20unilateral%20measures.pdf

Legislação espanhola, disponível em https://www.boe.es/boe/dias/2020/10/16/pdfs/BOE-A-2020-12355.pdf

Legislação europeia, disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A148%3AFIN

Legislação europeia, disponível em https://research.ibfd.org/#/doc?url=/linkresolver/static/tt_e2_41_eng_2011_tt__ad7%23tt_e2_41_eng_2011_tt__ad7

Legislação francesa, disponível em https://www.impots.gouv.fr/sites/default/files/media/1_metier/5_international/french_dst_en_v2.pdf?l=en

Legislação húngara, disponível em https://net.jogtar.hu/jogszabaly?docid=a1400022.tv

Legislação indiana, disponível em https://www.incometaxindia.gov.in/pages/acts/equalisation-levy.aspx (12.05.2022)

Legislação queniana, disponível em http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=CAP.%20470#part_II, e http://www.parliament.go.ke/sites/default/files/2022-04/The%20Finance%20Bill%2C%202022-1.pdf

Legislação turca, disponível em https://www.resmigazete.gov.tr/eskiler/2022/05/20220531-7.htm

Li, Jinyan, "The Legal Challenges of Creating a Global Tax Regime with the OECD Pillar One Blueprint", *in Bulletin for International Taxation*, Volume 75, n.º2, 2021, disponível em http://link.library.ibfd.org/portal/The-legal-challenges-of-creating-a-global-tax/qEVH9CqDUxA/

OCDE, "Addressing the Tax Challenges of the Digital Economy: Inclusive Framework on BEPS", *in OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing*, disponível em https://www.oecd.org/tax/addressing-the-tax-challenges-of-the-digital-economy-action-1-2015-final-report-9789264241046-en.htm

OCDE, "Tax Challenges Arising from Digitalisation – Report on Pillar One Blueprint: Inclusive Framework on BEPS*", in OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing*, disponível em https://www.oecd.org/tax/beps/tax-challenges-arising-from-digitalisation-report-on-pillar-one-blueprint-beba0634-en.htm

OCDE, "Tax Challenges Arising from Digitalisation – Report on Pillar Two Blueprint: Inclusive Framework on BEPS", *in OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing,* disponível em https://www.oecd.org/tax/beps/tax-challenges-arising-from-digitalisation-report-on-pillar-two-blueprint-abb4c3d1-en.htm

OCDE, Ker, Daniel, Mazzini, Emanuele, "Perspectives On The Value Of Data And Data Flows", *in OECD Digital Economy Papers*, 2020, disponível em https://www.oecd-ilibrary.org/docserver/a2216bc1-en.pdf?expires=1646309134&id=id&accname=guest&checksum=7D020ED210C6B8C2F19E9A09E1A081FE

OECD, "Progress Report On Amount A Of Pillar One - Two-Pillar Solution To The Tax Challenges Of The Digitalisation Of The Economy: Inclusive Framework", *in OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing,* disponível em https://www.oecd.org/tax/beps/progress-report-on-amount-a-of-pillar-one-two-pillar-solution-to-the-tax-challenges-of-the-digitalisation-of-the-economy.htm

OECD, "Tax Challenges Arising from Digitalisation – Interim Report 2018: Inclusive Framework on BEPS", *in OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing*, disponível em https://doi.org/10.1787/9789264293083-en

P. Burg, France - Corporate Taxation, *in Country Tax Guides IBFD*, disponível em https://research.ibfd.org/#/doc?url=/document/cta_fr_s_14 (12.05.2022)

Proposta legislativa europeia, disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018PC0147

Rawal, Radhakishan, Agarwal, Madhu, "Pillar One and Pillar Two", *in Deloitte*, disponível em https://www2.deloitte.com/content/dam/Deloitte/in/Documents/tax/in-tax-pillar-one-and-pillar-two-noexp.pdf

Regulamento Geral sobre a Proteção de Dados, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679

S. Shah, India - Corporate Taxation, *in Country Tax Guides IBFD*, disponível em https://research.ibfd.org/#/doc?url=/document/cta_in_s_2 (12.05.2022)

Sarfo, Nana, "Stakeholders' Deep Dive Into Amount A In-Scope Rules*", in Journal Articles & Opinion Pieces Tax Analysts*, disponível em https://www.taxnotes.com/tax-notes-today-international/international-taxation/stakeholders-deep-dive-amount-scope-rules/2022/05/23/7dhnj

Sítio na Internet da WIPO, disponível em https://wipolex.wipo.int/en/text/283693

Sítio na Internet da WIPO, disponível em https://www.wipo.int/edocs/pubdocs/en/wipo_pub_450_2020.pdf

Trakman, Leon, Walters, Roberts, Zeller, Bruno, "Is Privacy and Personal Data Set to Become the New Intellectual Property?", *in UNSW Law Research Paper*, n.º 19-70, 2019, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3448959

Y. Schuchter & A. Kras, Austria - Corporate Taxation, *in Country Tax Guides IBFD,* disponível em https://research.ibfd.org/#/doc?url=/document/cta_at_s_14 (12.05.2022)

O REGIME EUROPEU DA MANIPULAÇÃO DE MERCADO E AS TRANSAÇÕES ORGANIZADAS NAS REDES SOCIAIS

José Luís Ferreira Teixeira

zelft98@gmail.com

Resumo: Os inéditos acontecimentos de 2021 em torno das ações da *GameStop* e que viriam a originar o fenómeno das "ações *meme*", provocaram uma grande volatilidade e resultaram em elevados prejuízos financeiros para investidores de retalho e profissionais. Estes acontecimentos revelaram o potencial das práticas coordenadas nas redes sociais para influenciar os preços nos mercados financeiros. Como tal, nesta dissertação, tendo como pano de fundo os acontecimentos referidos, analisam-se as práticas de negociação coordenada de investidores de retalho através das redes sociais à luz dos objetivos prosseguidos pelo Direito para os mercados financeiros, bem como a aplicabilidade do regime europeu da manipulação de mercado do MAR a tais práticas. Concluímos que estas práticas coordenadas têm o potencial para produzir efeitos semelhantes aos da tradicional manipulação de mercado, contrariando os objetivos da regulação dos mercados financeiros e o conceito de bons mercados que o Direito procura proteger e que o regime europeu da manipulação de mercado é, apenas de forma muito limitada, aplicável a estas práticas.

Palavras-chave: Manipulação de mercado; transações coordenadas; redes sociais; investidores de retalho; MAR

Abstract: The unprecedented events of 2021 surrounding GameStop stock, which eventually led to the "meme stock" phenomenon, caused high volatility and resulted in large financial losses for retail and professional investors. These events revealed the potential of coordinated practices on social networks to influence prices in financial markets. As such, in this dissertation, with the aforementioned events as a backdrop, we analyze the coordinated trading practices of retail investors through social networks in light of the objectives pursued by the Law for financial markets, as well as the applicability of MAR's European market manipulation regime to such practices. We conclude that these coordinated practices have the potential to produce effects similar to traditional market manipulation, contrary to the objectives of financial market regulation and the concept of good markets which the law seeks to protect, and that the European market manipulation regime is only to a very limited extent applicable to these practices.

Keywords: Market manipulation; coordinated trading; social networks; retail investors; MAR

1. INTRODUÇÃO

No início do ano de 2021, nos Estados Unidos da América, os mercados financeiros mais desenvolvidos a nível mundial, foram palco de uma prática inédita na história dos mercados financeiros, que provocou uma influência de grandes proporções no preço das ações da empresa *GameStop*.

Um grande número de pequenos investidores de retalho em interação através das redes sociais e com um objetivo de manifestarem o seu descontentamento perante as posições a descoberto nas ações da *GameStop* (manifestação de emoções) desenvolveram uma estratégia de negociação coordenada que levou cada participante da estratégia a negociar nos mercados financeiros de acordo com as instruções discutidas nas redes sociais. Tal levou a uma hipervalorização do preço da *GameStop* em relação ao seu valor fundamental, o que, por sua vez, levou ao *short squeeze* de fundos de investimento de alto retorno com vendas a descoberto das ações da *GameStop*, sendo estes obrigados a fechar as suas posições de negociação com perdas muito elevadas. A elevada volatilidade dos preços provocou também perdas a investidores de retalho envolvidos e não envolvidos na prática coordenada. No seguimento do caso, os investidores de retalho nas redes sociais voltaram as atenções para outras empresas dadas como sem potencial e, como tal, alvo de vendas a descoberto. As ações de empresas em tal situação viriam a ser apelidadas de "ações *meme*".

Os mercados financeiros desempenham funções de elevada importância, permitindo a canalização de poupanças e investimento para a economia de modo a facilitar a acumulação de capital e a produção de bens e serviços, v.g., fornecendo capital de investidores que permitirá a empresas investir e concretizar projetos (os quais podem criar mais postos de trabalho), enquanto permitem aos investidores obter lucros do seu investimento. Bons mercados financeiros fomentam o crescimento económico e a criação de postos de trabalho, e como tal a sua integridade e a confiança nos mesmos deve ser protegida.

Olhando às consequências do caso *GameStop* e ao evidenciado potencial de práticas de negociação coordenada nas redes sociais para obter um número indefinido de participantes e influenciar preços de instrumentos financeiros mediante a introdução de modificações nos mecanismos de formação dos preços, impera analisar a negociação coordenada de investidores de retalho através das redes sociais no sentido de apurar se estas são compatíveis com os objetivos dos mercados financeiros prosseguidos pelo Direito, e se podem constituir manipulação de mercado à luz do regime europeu de manipulação de mercado.

Como tal, esta dissertação incide na análise da negociação coordenada de investidores de retalho através das redes sociais em mercados financeiros.

Ou seja, a negociação dos investidores de retalho participantes (compra, venda ou manutenção de instrumentos financeiros) de acordo com a estratégia definida e coordenada através de publicações nas redes sociais com o objetivo de influenciar os preços de modo a expressar uma opinião ou emoção.

Na nossa dissertação iremos quando necessário utilizar os conceitos da teoria económico-financeira necessários a uma melhor compreensão dos problemas em questão, seguindo as palavras de Emilios Avgouleas, o qual aponta que «uma sólida compreensão dos mercados financeiros modernos e dos conceitos de teoria económica utilizados para os explicar é indispensável no estudo do abuso de mercado».[1]

Começaremos, no primeiro capítulo (2. O caso *GameStop* e a génese da negociação coordenada de investidores de retalho através das redes sociais), por descrever a génese da negociação coordenada dos investidores de retalho nas redes sociais através do caso *GameStop*, descrevendo os fatores-chave do mesmo, os quais serão importantes na análise subsequente. De seguida, procederemos à delimitação do conceito de negociação coordenada de investidores de retalho através das redes sociais.

No segundo capítulo (3. Os objetivos da regulação dos mercados financeiros e a negociação coordenada nas redes sociais), começaremos por analisar o objetivo da regulação dos mercados financeiros e as características que se pretendem em bons mercados financeiros. Para a compreensão do funcionamento de bons mercados financeiros e da sua eficiência, procederemos à necessária introdução dos fundamentos básicos da teoria financeira que estão na base das soluções legais, passando pelo conceito de valor fundamental à luz do conceito de eficiência seguido. Tentamos até aqui perceber não só os objetivos e características dos mercados financeiros que o Direito adota, mas também o mecanismo de formação de preços e interação entre procura e oferta de modo a compreender em que medida a negociação coordenada poderá interferir com os últimos. Terminaremos o capítulo com a ponderação e comparação dos conceitos e consequências da manipulação de mercado e da negociação coordenada de investidores de retalho nas redes sociais, concluindo acerca de uma possível compatibilidade das práticas de negociação coordenada de investidores de retalho através redes sociais com a manipulação de mercado de um ponto de vista conceptual e das consequências produzidas.

No terceiro capítulo (4. A manipulação de mercado do MAR), procederemos a uma breve exposição e caracterização do Regulamento do Abuso de Mercado (*Market Abuse Regulation,* doravante MAR) que regula a manipula-

[1] «A sound understanding of modern financial markets and of economic theory concepts used to explain them is indispensable in the study of market abuse. » Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 22.

ção de mercado na União Europeia, bem como do regime da manipulação de mercado que o referido regulamento contém.

No quarto capítulo (5. A negociação coordenada dos investidores de retalho através das redes sociais), a análise detalhada incidirá nas efetivas transações levadas a cabo pelos investidores de retalho no âmbito da NCIRRS enquanto passível de submissão da alínea a) do número 1 do artigo n.º 12.º do MAR e da alínea a) do número 2 do artigo 12.º do mesmo regulamento.

No quinto capítulo (6. As publicações da negociação coordenada nas redes sociais) analisaremos detalhadamente a possibilidade de aplicação das alíneas c) e b) do número 1 do artigo 12.º do MAR às publicações nas redes sociais no âmbito da negociação coordenada de investidores de retalho nas redes sociais.

Por fim, estaremos em condições de concluir acerca da compatibilidade das práticas da negociação coordenada de investidores de retalho através das redes sociais com os objetivos da regulação dos mercados financeiros, com o conceito de bons mercados (que o Direito procura proteger) e com o tradicional conceito de manipulação de mercado; bem como se estas podem constituir manipulação de mercado à luz do regime europeu de manipulação de mercado.

Em suma, esta dissertação foca-se essencialmente na análise das práticas de negociação coordenada dos investidores de retalho através das redes sociais à luz dos objetivos prosseguidos pelo Direito para os mercados financeiros, bem como na aplicabilidade do regime europeu da manipulação de mercado do MAR a tais práticas. Essa análise abrange as condutas delimitadas pelo nosso conceito de negociação coordenada de investidores de retalho, as quais incidem em mercados financeiros. A dissertação limitará a análise dos problemas ao plano europeu, visto que o Regulamento do Abuso de Mercado tem aplicação direta no espaço da União Europeia, não podendo os Estados-Membros desviar-se das normas estabelecidas no referido regulamento em consequência da harmonização total vigente na União Europeia em matérias de abuso de mercado. Também não analisaremos os casos do ponto de vista da responsabilidade criminal decorrente da infração das normas europeias no território dos Estados-Membros.

2. O CASO *GAMESTOP* E A GÉNESE DA NEGOCIAÇÃO COORDENADA DE INVESTIDORES DE RETALHO ATRAVÉS DAS REDES SOCIAIS

2.1. GAMESTOP

Nos Estados Unidos da América, um pequeno grupo de investidores não profissionais de baixo poder financeiro, entre os quais se destacou Keith Gill, focaram a sua atenção nas ações da empresa *GameStop* (doravante, GME).

Keith Gill começou a adquirir ações da GME em junho de 2019, quando cada ação estava cotada em cerca de 5 dólares americanos[2]. A GME apresentava, na altura, dificuldades em acompanhar o desenvolvimento dos seus concorrentes de negócio digital, o que a tornava, à data, pouco popular perante os investidores, dadas as baixas expectativas de lucro financeiro[3]. Keith Gill promoveu o seu investimento nas redes sociais, acreditando que a empresa tinha capacidade para inverter a difícil situação e se valorizar novamente, o que fez com que seja considerado como a figura que iniciou a discussão nas redes sociais no caso GME. Destaca-se a rede social *Reddit*, nomeadamente, o seu fórum *WallStreetBets* (doravante WSB), que conta com milhões de membros, onde os pequenos investidores partilham e discutem sobre investimentos.[4]

a) As vendas a descoberto

Enquanto os pequenos investidores discutiam nas redes sociais sobre a empresa GME, fundos de retorno absoluto (*hedge funds*), tal como a *Melvin Capital Management* e a *Citron Research*, especializados em descobrir empresas com um preço de mercado superior ao seu valor fundamental[5] - sobrevalorizado segundo os fundamentos de finanças - detinham posições de venda a descoberto[6]. Por outras palavras, venderam ações que não possuíam, mas receberam através de um empréstimo, esperando lucrar quando o mercado ajustasse o preço das ações àquilo que estas realmente valessem, comprando nesse momento as ações ao preço mais baixo e lucrando com a diferença entre o preço a que compraram e o preço a que venderam[7]. A GME chegou a ter um interesse de venda a descoberto (*short)* de 140%, o que significa que por cada ação da empresa, havia 1,4 ações vendidas a

2 Julia-Ambra Verlaine e Gunjan Banerji, "Keith Gill Drove the GameStop Reddit Mania. He Talked to the Journal", Wall Street Journal, disponível em: https://www.wsj.com/articles/keith-gill-drove-the-GameStop-reddit-mania-he-talked-to-the-journal-11611931696 (consultado em 21 de junho de 2022).

3 Matt Levine, "The GameStop Game Never Stops", Bloomberg, disponível em: https://www.bloomberg.com/opinion/articles/2021-01-25/the=-game-never-stops?sref-1kJVNqnU (consultado em 21 de junho de 2022).

4 Ibid.

5 Ver *infra*, capítulo II 3.

6 A venda a descoberto é uma técnica utilizada quando se acredita que os preços de um instrumento financeiro se encontram sobrevalorizados. John Armour et al., *Principles of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015, p. 195 e ss. Ver ainda António Barreto Menezes Cordeiro, Manual de Direito dos Valores Mobiliários, 2ª edição, Coimbra, Almedina, 2019, pp. 210-212. Paulo Câmara, *Manual de direito dos valores mobiliários*, 4ª edição, Coimbra, Almedina, 2018, pp. 205-218. Zvi Bodie, Alex Kane e Alan Marcus, Investments, 11ª edição, New York, McGraw-Hill Education, 2018, pp. 78-82.

7 Jonathan Macey, "Securities Regulation Warfare", *Columbia Business Law Review*, 2021, p.4 disponível em: https://ssrn.com/abstract=3789706.

descoberto[8], ou seja, mais ações vendidas a descoberto do que aquelas que existiam no mercado.

b) A reação coordenada dos pequenos investidores

Assim que os pequenos investidores da comunidade WSB tomaram conhecimento das volumosas posições a descoberto em ações da GME, assumiram uma posição contra os fundos de retorno absoluto, pretendendo "derrubar" estes fundos[9]. Os investidores nas redes sociais sinalizaram o seu empenho obstinado em comprar e manter as ações através do *meme* "*Diamond Hands*"[10], que é um termo usado como metáfora para um investidor de longo prazo num ativo popular, apesar de todas as rápidas oscilações dos preços[11]. Os pequenos investidores estimularam-se mutuamente através das redes sociais, nomeadamente, nas redes *Reddit*, *Twitter* e *YouTube*, e sinalizaram uma visão extrema da potencial valorização através do *meme* "foguetão"(*Rocket*)[12].

As cotações da GME subiram ainda mais quando Elon Musk, um dos mais influentes e bem-sucedidos empresários norte-americanos, publicou na rede social *Twitter* uma ligação para o sítio da rede *Reddit* que hospedava os investidores de retalho mais atentos à GME - o *WallStreetBets*[13], atraindo ainda mais investidores para este subfórum da rede *Reddit*. Aumentou assim, ainda mais, o potencial de disseminação e propagação da estratégia dos investidores de retalho.

Esta ação coletiva dos pequenos investidores do grupo WSB representou uma tentativa de fazer frente aos ricos e poderosos investidores profissionais, nomeadamente os grandes fundos de investimento[14]. Através da

---

8 Katherine Greifeld e Lu Wang, "GameStop Short Interest Plunges in Sign Traders Are Covering", Bloomberg, disponível em: https://www.bloomberg.com/news/articles/2021-02-01/gamestop-short-interest-plummets-in-a-sign-traders-are-covering (consultado em 21 de junho de 2022).

9 Ibid.

10 Este meme consiste numa imagem onde sejam apresentadas mãos a segurar um ou mais diamantes.

11 Gonçalo Almeida, "Lembra-se da GameStop ou da AMC? As "meme stocks" continuam a dar que falar em Wall Street", Jornal de Negócios, disponível em: https://www.jornaldenegocios.pt/mercados/detalhe/lembra-se-da-gamestop-ou-da-amc-as-meme-stocks-continuam-a-dar-que-falar-em-wall-street (consultado em 21 de junho de 2022).

12 Lasse Pedersen, *Game On: Social Networks and Markets*, NYU Stern School of Business, p.26, disponível em: https://ssrn.com/abstract=3794616.

13 Shalini Nagarajan, "GameStop explodes another 157% higher after Elon Musk's 'Gamestonk' tweet extends Reddit-driven short squeeze", Business Insider, disponível em: https://markets.businessinsider.com/news/stocks/gamestop-stock-price-elon-musk-gamestonk-tweet-extends-trading-rally-2021-1-1030009065 (consultado em 21 de junho de 2022).

14 Jonathan Macey, "Securities Regulation Warfare", *Columbia Business Law Review*, 2021, p. 4, disponível em: https://ssrn.com/abstract=3789706 .

negociação sob lemas como "*YOLO*"[15] (*you only live once*), os pequenos investidores adquiriam as ações e tentavam segurá-las, não vendendo independentemente da movimentação do curso das ações.

O curso das ações da GME subiu 1500% durante o mês de janeiro de 2021, atingindo um preço superior a 320 dólares por ação[16]. Os especialistas avaliavam a GME em 2 mil milhões de dólares. Os pequenos investidores impulsionaram o valor da empresa até aos 23 mil milhões de dólares[17], no dia 27 de janeiro de 2021. O curso das ações aumentou até aos 2500% em janeiro, caiu de seguida drasticamente, e aumentou novamente, tendo os picos associados ao volume e volatilidade de negociação coincidido com um aumento da atenção nas redes sociais e outros *media*[18]. O volume diário de negociação atingiu um pico acima dos 200% a 22 de janeiro, o que significa que todas as ações da empresa foram negociadas mais de duas vezes por dia[19], em demonstração da imensa atividade que decorreu no referido pico.

c) Aquisição de valores mobiliários e instrumentos derivados financeiros

Os investidores de retalho "apostaram" na GME através da aquisição de ações e de opções. As opções são contratos que conferem ao adquirente (posição longa) o direito de, até uma específica data, poder acionar uma cláusula que lhe permite comprar ou vender[20] as respetivas ações ao preço fixado no contrato[21]. Estes instrumentos financeiros derivados incorporam

---

15 Lasse Pedersen, "Game On: Social Networks and Markets", *NYU Stern School of Business*, 2021, p. 26, disponível em: https://ssrn.com/abstract=3794616.

16 Harry Robertson, "Short-Sellers Are Nursing Estimated Losses Of $19 Billion in 2021 After Betting on GameStop's Stock to Plunge", Business Insider, https://markets.businessinsider.com/news/stocks/short-sellers-sitting-on-19-billion-of-losses-on-GameStop-data-shows-2021-1-1030020684 (consultado em 21 de junho de 2022).

17 Olga Kharif, "What's the $23 Billion GameStop Really Worth? Maybe $2 Billion", Bloomberg,https://www.bloomberg.com/news/articles/2021-01-27/what-s-the-23-billion-gamestop-really-worth-maybe-2-billion (consultado em 21 de junho de 2022).

18 Lasse Pedersen, "Game On: Social Networks and Markets", *NYU Stern School of Business*, 2021, p. 5, disponível em: https://ssrn.com/abstract=3794616.

19 Lasse Pedersen, "Game On: Social Networks and Markets", *NYU Stern School of Business*, 2021, p. 30, disponível em: https://ssrn.com/abstract=3794616.

20 Conforme se trate de uma opção de compra (*call option*) ou de uma opção de venda (*put option*).

21 Zvi Bodie, Alex Kane e Alan Marcus, Investments, 11ª edição, New York, McGraw-Hill Education, 2018, p. 50. Por outro lado, a parte que vende o contrato (posição curta) está obrigada a executar a venda ou compra se a parte com a posição longa exercer a cláusula de opção. A parte com a posição curta deve possuir os instrumentos financeiros na base do contrato para o caso de a parte longa decidir exercer a opção. Tal necessidade de possuir os instrumentos financeiros na base do contrato é expressa no rácio de cobertura. Zvi Bodie, Alex Kane e Alan Marcus, Investments, 11ª edição, New York, McGraw-Hill Education, 2018, p. 50.

De um ponto de vista económico-financeiro, são contratos cujo exercício do direito conferido apenas compensa se os preços das ações subjacentes nos diversos locais

alavancagem, permitindo aos investidores multiplicar muitas vezes os seus ganhos ou perdas para o mesmo investimento[22].

Quando os investidores finais (posição longa) adquirem opções de compra, estas são, normalmente, vendidas por criadores de mercado (posição curta) que cobrem o seu risco comprando as ações que constam no contrato de opção, precavendo-se para o caso de a sua contraparte decidir exercer a opção[23]. O rácio de cobertura (o *delta*) aumenta conforme o preço das ações se movimente num sentido favorável ao exercício da opção de compra. Esta alteração no rácio de cobertura, por sua vez, é chamada de *gamma*[24]. Deste modo, um aumento do preço das ações leva a parte com posição curta num contrato de opção de compra a adquirir as mesmas para poder cumprir com o mesmo, cobrindo o seu risco para o caso de os investidores acionarem a opção de compra das ações. Para estes compensará acionar a opção de compra se os preços das ações forem superiores ao preço a pagar através da ativação da opção[25]. Estas compras provocam uma pressão acrescida na procura, o que leva a novos aumentos do preço das ações e estes, por sua vez, levam a aumentos do rácio de cobertura, dando-se um aperto *gamma* (*gamma squeeze)*. Assim, a compra de opções é comparável a uma estratégia de transação pré-programada, em que o investidor final compra cada vez mais ações à medida que o preço sobe[26], devido ao facto de a contra-

de negociação forem superiores ao preço fixado para o exercício pelo direito de compra. Inversamente, opções de venda são contratos cuja opção de venda conferida apenas compensa sob um ponto de vista económico-financeiro se o preço de venda nos diversos locais de negociação for inferior ao preço de venda fixado na cláusula de opção do contrato. Zvi Bodie, Alex Kane e Alan Marcus, Investments, 11ª edição, New York, McGraw-Hill Education, 2018, pp. 50 e ss.

A opção conferida pelo contrato de opção «representa um direito, mas não uma obrigação, a adquirir ou dispor de um bem ou a celebrar um contrato em data futura.» Paulo Câmara, *Manual de direito dos valores mobiliários*, 4ª edição, Coimbra, Almedina, 2018, p. 212. Sobre instrumentos financeiros derivados ver também António Barreto Menezes Cordeiro, Manual de Direito dos Valores Mobiliários, 2ª edição, Coimbra, Almedina, 2019, pp. 215-251.

22 Lasse Pedersen, "Game On: Social Networks and Markets", *NYU Stern School of Business*, 2021, p. 32, disponível em: https://ssrn.com/abstract=3794616.

23 Ibid. Tal necessidade da parte com a posição curta de se precaver para a possibilidade de a parte com a posição longa exercer a opção está expressa no rácio de cobertura.

24 Ibid.

25 Por exemplo, se um investidor tiver adquirido um contrato de opção de compra europeu de ações de uma determinada empresa com preço de opção de 10 euros por ação e na data de fim de contrato as ações em mercado secundário tiverem o preço de 12 euros, então este irá exercer a opção. Os contratos de opções europeus distinguem-se dos americanos, na medida em que nos primeiros o investidor só pode exercer a opção na data de fim de contrato. Já nos americanos, pode-se exercer a qualquer altura, desde que até à data de fim do contrato. Sobre isto, Zvi Bodie, Alex Kane e Alan Marcus, Investments, 11ª edição, New York, McGraw-Hill Education, 2018, p. 661.

26 Ibid.

parte central ter de comprar ações para cobrir o risco e poder cumprir a sua parte do contrato.

À medida que o preço das ações da GME subiu no final de janeiro, alguns detentores de posições a descoberto foram, a fim de reduzirem os seus prejuízos, obrigados a fechar as suas posições, comprando ações que anteriormente lhes tinham sido emprestadas para a realização das vendas a descoberto[27]. Esta redução nas posições curtas através da compra de ações colocou ainda maior pressão do lado da procura em relação à oferta, provocando uma maior subida do preço, em sentido contrário ao das posições de venda a descoberto - *short squeeze*[28], uma vez que aumentou a procura em relação à oferta. Como consequência dos *short squeeze* e *gamma squeeze*, alguns fundos de investimento de retorno absoluto sofreram perdas na ordem dos milhares de milhões de dólares, nomeadamente a *Melvin Capital Management* com perdas de 53% no mês de janeiro, tendo vindo, como consequência, a necessitar de injeções de capital de quase 3 mil milhões de dólares.[29] Mas não só os grandes fundos de capitais sofreram grandes perdas, resultando a elevada volatilidade[30] também em avultados prejuízos do lado dos pequenos investidores de retalho.[31]

Assim, esta oscilação do preço das ações da GME criou e destruiu cerca de 30 mil milhões de dólares de capital, afetando várias classes de investidores, causando perdas não só a investidores profissionais, mas também a investidores de retalho envolvidos no esquema com o fim de contrariar os grandes fundos de investimento, bem como a investidores de retalho que apenas pretendiam retirar lucros financeiros. [32]

d) Os fatores estimuladores

Os acontecimentos do caso GME foram facilitados sobretudo pelas interações nas redes sociais e pela facilidade em negociar instrumentos finan-

---

[27] Katherine Greifeld e Lu Wang, "GameStop Short Interest Plunges in Sign Traders Are Covering", Bloomberg, disponível em: https://www.bloomberg.com/news/articles/2021-02-01/gamestop-short-interest-plummets-in-a-sign-traders-are-covering (consultado em 21 de junho de 2022).

[28] Lasse Pedersen, "Game On: Social Networks and Markets", *NYU Stern School of Business*, 2021, p. 32, disponível em: https://ssrn.com/abstract=3794616.

[29] Colin Keatinge, "Melvin Lost 53% in January, Hurt by GameStop, Other Bets", Bloomberg, disponível em: https://www.bloomberg.com/news/articles/2021-01-31/melvin-lost-53-in-january-hurt-by-gamestop-other-bets-dj (consultado em 21 de junho de 2022).

[30] Entre janeiro e fevereiro deu-se uma acentuada queda dos preços - a GameStop apresentava um curso de 40 dólares americanos em meados de fevereiro de 2021.

[31] Rachel Ensign, "GameStop Investors Who Bet Big—and Lost Big", Wall Street Journal, disponível em: https://www.wsj.com/articles/gamestop-investors-who-bet-bigand-lost-big-11613385002 (consultado em 21 de junho de 2022).

[32] Matt Phillips *et al*., "The Hopes That Rose And Fell With GameStop", New York Times, disponível em: https://www.nytimes.com/2021/02/07/business/gamestop-stock-losses.html (consultado em 11 de abril de 2022)

ceiros através de intermediários financeiros com serviços de corretagem sem comissões, que disponibilizam o seu serviço online, ou em aplicações de *smartphone* de interface simples e, em muitos casos, "gamificada"[33], sendo que o aumento de tempo disponível devido ao confinamento provocado pela primeira vaga da pandemia da covid-19 constituiu também um importante catalisador[34].

e) As meme stocks

Lasse Pedersen considera que o *short squeeze* desempenhou um grande papel no pico dos preços em janeiro, mas que, por outro lado, não foi um fator no subsequente aumento dos preços em março[35], o que releva a importância dos efeitos das negociações coordenadas nas redes sociais e do seu potencial de estabelecimento enquanto prática no futuro.

Efetivamente, tem-se verificado que o fenómeno da compra massiva de ações, organizada e coordenada nas redes sociais, se desenvolveu, alargando os investidores de retalho o seu âmbito de compra de ações a outras empresas desvalorizadas e em queda, e como tal, com grande interesse para vendas a descoberto, tais como a *AMC Entertainment Holdings*, a *Blackberry* ou a *Nokia*. Consequentemente, estas continuaram com cotações sobrevalorizadas e volumes de transações bastante elevados[36]. Estes acontecimentos viriam apenas a ser o início daquilo que foi denominado o fenómeno das *meme stocks* ("ações *meme*"), i.e., ações cujo valor não se baseia em fundamentos de finanças, mas em interações e tendências das redes sociais que resultam em grandes oscilações dos preços nos mercados financeiros (elevadas volatilidades)[37].

A senadora norte-americana Elizabeth Warren escreveu, inclusive, uma carta à *Securities and Exchange Commission* (doravante SEC), a autoridade norte-americana de supervisão de mercados financeiros, na qual apelou a uma profunda investigação sobre os fenómenos mencionados, expressando

33 Lasse Pedersen, "Game On: Social Networks and Markets", *NYU Stern School of Business*, 2021, p. 26, disponível em: https://ssrn.com/abstract=3794616. Os elementos de *gamificação* consistem em elementos como fogo de artifício após a execução de cada ordem, tal como se o cliente tivesse completado um desafio num jogo. Estes verificam-se, v.g. na aplicação da corretora *Robinhood.* Annie Massa e Tracy Alloway, "Robinhood's Role in the 'Gamification' of Investing", Bloomberg, disponível em: https://www.bloomberg.com/news/articles/2020-12-19/robinhood-s-role-in-the-gamification-of-investing-quicktake

34 Jim Bianco, "Wall Street Never Saw the Redditors Coming", Bloomberg, disponível: https://www.bloomberg.com/opinion/articles/2021-02-02/wall-street-didn-t-see-reddits-wallstreetbets-coming-for-gamestop-gme (consultado em 21 de junho de 2022)

35 Lasse Pedersen, "Game On: Social Networks and Markets", *NYU Stern School of Business*, 2021, p. 32, disponível em: https://ssrn.com/abstract=3794616.

36 Matt Levine, "The Meme Stocks keep coming", Bloomberg, available at: https://www.bloomberg.com/opinion/articles/2021-06-09/the-meme-stocks-keep-coming (consultado em 21 de junho de 2022).

37 Ibid.

preocupação acerca das consequências que os fenómenos recentes poderiam ter na confiança da sociedade nos mercados e sublinhando a importância de ter mercados financeiros justos, ordeiros e eficientes[38]. A proteção da função dos mercados financeiros e da confiança nos mesmos por parte dos investidores são, como iremos ver, objetivos da regulação dos mercados financeiros também na União Europeia.

Se os acontecimentos iniciais com as ações da GME já seriam suficientes, isoladamente, para levantar questões relacionadas com a regulação dos mercados financeiros, o facto de as práticas de negociação coordenadas através das redes sociais serem persistentes e terem grande volume nos mercados de capitais e de derivados aumentou consideravelmente o número de questões legais e económico-financeiras.

f) As primeiras conclusões da autoridade norte-americana de supervisão dos mercados de valores mobiliários (SEC) e a resposta académica

A SEC publicou em outubro de 2021 um relatório onde argumenta que os investidores (institucionais) que fecharam as suas posições a descoberto nas ações da GME através da compra das respetivas ações desempenharam apenas um papel menor no desenvolvimento deste caso. Apesar de os reguladores americanos afirmarem não conseguir determinar, exatamente, o que provocou a extrema volatilidade dos preços das ações da GME, estes especularam apenas que a razão poderia ser o otimismo dos investidores em relação às perspetivas da empresa, ou o facto de estes acreditarem poder desencadear um *short squeeze*.[39]

Em resposta ao relatório da SEC, um grupo de académicos das áreas do Direito e das Finanças de algumas das mais reputadas universidades norte-americanas, criticaram a perspetiva apresentada no relatório. Num estudo de 28 de janeiro de 2022[40], afirmaram que a análise dos factos realizada pela SEC resultou de uma utilização incompleta de dados e de métodos defeituosos, chegando a conclusões erróneas acerca dos eventos e que, consequen-

38 Elizabeth Warren, Letter to the Acting Chair of the U.S. Securities and Exchange Commission (SEC), United States Senate, 2021. Disponível em: https://www.warren.senate.gov/imo/media/doc/01.29.2021%20Letter%20from%20Senator%20Warren%20to%20Acting%20Chair%20Lee.pdf (consultado em 21 de junho de 2022).

39 Matt Robinson, "Meme-Stock Frenzy Gets a Fresh Look That Questions SEC Narrative", Bloomberg, disponível em: https://www.bloomberg.com/news/articles/2022-02-14/meme-stock-frenzy-gets-a-fresh-look-that-questions-sec-narrative (consultado a 17 de junho de 2022).

40 Joshua Mitts *et al*., A Report by the Ad Hoc Academic Committee on Equity and Options Market Structure Conditions in Early 2021, 28 janeiro de 2022, disponível em: https://ssrn.com/abstract=4030179

temente, a sua resposta ao referido caso e às "ações *meme*" poderia estar profundamente mal orientada[41].

Joshua Mitts, o líder do referido grupo de académicos, afirmou que os episódios do caso GME e das "ações *meme*" expôs a fragilidade do mercado a esquemas que podem provocar a negociação de ações a preços afastados do seu valor fundamental, que não refletem os rendimentos das empresas. Neste tipo de cenário, um ajustamento dos preços ao seu valor fundamental pode provocar enormes prejuízos aos investidores posicionados do lado errado da reação.[42] Joshua Mitts defende que as normas de manipulação de mercado americanas devem ser ajustadas de modo a serem aptas a responder à nova era das redes sociais.[43] No caso, os *short squeeze* e *gamma squeeze* provocados pela negociação coordenada nas redes sociais são prejudiciais à normal negociação e desenvolvimento do preço.[44]

2.2. A NEGOCIAÇÃO COORDENADA DE INVESTIDORES DE RETALHO ATRAVÉS DAS REDES SOCIAIS (NCIRRS)

a) O processo de coordenação da negociação nas redes sociais

Num artigo de 2021, Michele Costola *et al*. propõem uma descrição do processo de coordenação descentralizada que ocorre nas redes sociais, defendendo que este consiste em três ações principais: em primeiro lugar, uma população de investidores de retalho que discute abertamente nas redes sociais sobre ações tidas como populares; em segundo lugar, um grupo de investidores de retalho que partilha a crença de que um determinado preço de ações pode ser afetado pelas suas compras conjuntas, coordena nas redes sociais, através de publicações com imagens e *meme*s, a compra sincronizada de grandes quantidades dessas ações; terceiro, à medida que os volumes negociados dessas ações começam a aumentar, mais investidores começam a reparar nos sinais de compra colocados nas redes e meios de comunicação social[45]. Consequentemente, mais investidores, também mo-

---

41 Matt Robinson, "Meme-Stock Frenzy Gets a Fresh Look That Questions SEC Narrative", Bloomberg, disponível em: https://www.bloomberg.com/news/articles/2022-02-14/meme-stock-frenzy-gets-a-fresh-look-that-questions-sec-narrative (consultado a 17 de junho de 2022).

42 Joshua Mitts *et al*., A Report by the Ad Hoc Academic Committee on Equity and Options Market Structure Conditions in Early 2021, 28 janeiro de 2022, disponível em: https://ssrn.com/abstract=4030179

43 Matt Robinson, "Meme-Stock Frenzy Gets a Fresh Look That Questions SEC Narrative", Bloomberg, disponível em: https://www.bloomberg.com/news/articles/2022-02-14/meme-stock-frenzy-gets-a-fresh-look-that-questions-sec-narrative (consultado a 17 de junho de 2022).

44 Ibid.

45 Michele Costola, Matteo Iacopini, Carlo. Santagiustina, "On the "mementum" of Meme Stocks", 2021, disponível em: https://ssrn.com/abstract=3861779

vidos pelo medo de ficar de fora (um sintoma normalmente designado como *fear of missing out*, ou FOMO) começam a comprar as ações, o que cria um efeito de comboio através do qual os preços das ações e os volumes negociados disparam[46]. Este fator psicológico dos investidores é um dos aspetos apontados pelas finanças comportamentais para criticar a perspetiva de que os mercados financeiros são eficientes[47]. Como iremos ver adiante, o Direito segue a perspetiva da eficiência dos mercados eficientes, nomeadamente, a ECMH, assumindo que um investidor razoável tem como objetivo maximizar lucros ajustados aos riscos[48].

b) Negociação expressiva

A propósito do objetivo de negociação por motivos que não a obtenção de lucro, Anderson *et al*. introduziram o conceito de *negociação expressiva* - a negociação de instrumentos financeiros para fins de expressão política, social, ou estética[49]. Os "negociadores expressivos" sabem que o movimento do preço das ações que geram não reflete os fundamentos das ações, e que podem incorrer em perdas quando a provável correção dos preços ocorrer[50]. No entanto, consideram que os seus atos valem o risco de quaisquer perdas associadas. Entre as motivações destes negociadores podem estar as de prejudicar os poderosos e ricos fundos de retorno absoluto e prejudicar o sistema, a utilização do mercado como meio de "protesto"[51] ou outros motivos mais lúdicos ou estéticos, como v.g., a nostalgia[52].

c) A delimitação do conceito

A nosso ver, daqui resulta que a negociação coordenada de investidores de retalho através das redes sociais (doravante, NCIRRS) se trata da nego-

---

46 Ibid.

47 Sobre finanças comportamentais, ver Robert Shiller, *Irrational Exuberance*, 3ª edição, Princeton University Press, 2016.

48 Ver *infra*, Capítulo II 2.

49 John Anderson, Jeremy Kidd e George Mocsary, "Social Media, Securities Markets, and the Phenomenon of Expressive Trading", 25 Lewis & Clark L. Rev. 1223, 2022, p. 11, disponível em: https://ssrn.com/abstract=3834801, .

50 John Anderson, Jeremy Kidd e George Mocsary, "Social Media, Securities Markets, and the Phenomenon of Expressive Trading", 25 Lewis & Clark L. Rev. 1223, 2022, p. 12, disponível em: https://ssrn.com/abstract=3834801,.

51 Jedidajah Otte, "'Sending a Message': GameStop Investors on Why They Boaught Shares", The Guardian, disponível em: https://www.theguardian.com/business/2021/jan/28/sending-a-message-gamestop-investors-on-why-they-bought-shares (consultado em 21 de junho 2022).

52 Eamon Javers, "Republicans in Washington warn Wall Street: The GameStop Populists Are More Powerful than You Think", CNBC, disponível em: https://www.cnbc.com/2021/01/28/gamestop-republicans-warn-of-trump-style-populist-revolution.html (consultado em 21 de junho 2022).

ciação dos investidores de retalho participantes (compra, venda ou manutenção de instrumentos financeiros) de acordo com a estratégia definida e coordenada através de publicações nas redes sociais com o objetivo de influenciar os preços de modo a expressar uma opinião ou emoção.

Os participantes da NCIRRS são, em regra, os investidores de retalho, os quais são investidores não profissionais, dispondo, em regra de menores conhecimentos e experiência nos mercados financeiros e estando, como tal, expostos a maiores riscos[53].

A nossa análise divide, portanto, a negociação coordenada em dois momentos: (1) as publicações nas redes sociais que são suscetíveis de instigar e dar instruções para a prática da negociação coordenada de instrumentos financeiros por um número indefinido de investidores de retalho através dessas redes e (2) a concreta aplicação da estratégia e negociação de instrumentos financeiros pelos inúmeros investidores de retalho – a negociação coordenada através das redes sociais.

3. OS OBJETIVOS DA REGULAÇÃO DOS MERCADOS FINANCEIROS E A NEGOCIAÇÃO COORDENADA NAS REDES SOCIAIS

Uma das funções mais importantes dos mercados financeiros é a de fornecer informação sobre as projeções dos investidores relativas a futuros ganhos, estando os participantes dos mercados financeiros continuamente a atualizar as suas crenças acerca dos lucros futuros em resposta a novas informações[54]. Por isso, os preços a que são realizadas as transações nos mercados financeiros agregam informação sobre o valor esperado dos instrumentos financeiros negociados[55]. O preço de um instrumento financeiro deve refletir a soma do valor presente dos interesses futuros ou pagamentos de dividendos e do preço do instrumento financeiro à data na qual o investidor antecipa vendê-lo[56]. No momento da aquisição, os investidores realizam investimentos, um compromisso atual de dinheiro ou outros recursos, na expectativa de obter benefícios no futuro[57], ou seja, o investidor sacrifica

---

53 Como tal, aos intermediários financeiros são, pela DMIF II (Diretiva 2014/65/EU), impostos um maior número de deveres perante estes clientes não profissionais. Ver Niamh Moloney, *EU Securities and financial markets regulation*, 3ª edição, Oxford, Oxford University Press, 2016, pp. 352 a 354.

54 John Armour et al., *Principles of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015, p. 101.

55 Ibid.

56 John Armour et al., *Principles of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015, p 102.

57 Zvi Bodie, Alex Kane e Alan Marcus, Investments, 11ª edição, New York, McGraw-Hill Education, 2018, p. 1.

algo hoje para obter benefícios mais tarde. Se os preços das ações devem refletir a avaliação coletiva dos investidores sobre o desempenho atual de uma empresa e dos seus lucros futuros, tal faz com que o preço das ações suba quando o mercado está mais otimista em relação à empresa, fazendo com que esta tenha mais facilidade em obter capital e encorajar o investimento[58]. Desta maneira, os preços dos valores mobiliários têm uma grande importância na alocação de capital nas economias de mercado, dirigindo capital para as empresas com maior potencial previsto[59].

Como exposto no caso GME, que veio a evoluir para o fenómeno das "ações *meme*", estas negociações coordenadas nas redes sociais, e que envolvem grandes números de investidores de retalho, levam a fortes implicações nos processos de formação dos preços e alocação de capitais, conduzindo a preços que não são totalmente formados à luz dos fundamentais das finanças. Acrescenta-se o facto de este tipo de transações realizadas pelos pequenos investidores de retalho poderem ter como objetivo não o investimento, mas uma expressão de um sentimento ou pretensão que não a de obtenção de um lucro financeiro (negociação expressiva[60]). No caso GME, o objetivo foi, em larga parte, provocar a subida do curso das ações de modo a prejudicar os fundos de investimento de alto retorno (*hedge funds)* que detinham posições de venda a descoberto, levando a prejuízos enormes destes últimos, os quais detinham posições legítimas visto que a empresa estava subvalorizada e com um modelo de negócio ultrapassado e, portanto, sem expectativas de poder vir a justificar o preço das suas ações.

É relevante realçar que as vendas a descoberto são defendidas por vários economistas como constituindo um mecanismo de aumento da eficiência do mercado através de um melhor ajuste dos preços, neste caso contribuindo para uma mais rápida exposição de cotações sobrevalorizadas e consequente ajuste dos preços ao seu valor fundamental.[61] É também, no entanto, importante sublinhar que estes mecanismos de mercado devem ser devidamente regulados de modo a evitar a sua utilização para fins de especulação que nada beneficiam a eficiência da descoberta do preço de um instrumento financeiro e que podem criar riscos sistémicos que prejudicam a estabilidade financeira e a confiança nos mercados. Estas matérias são reguladas na União Europeia através do Regulamento das Vendas a Descoberto[62]. Por outro lado, o objetivo inicial de muitos dos investidores de retalho de prejudicar os grandes fundos de retorno absoluto evoluiu para o fenóme-

58 Zvi Bodie, Alex Kane e Alan Marcus, Investments, 11ª edição, New York, McGraw-Hill Education, 2018, p. 5.

59 Ibid.

60 Ver *supra*, Capítulo I 2.2.

61 Edward Miller, "Risk, Uncertainty and Divergence of Opinion", *The Journal of Finance,* Vol. 32, n.º 4, 1977, p. 1151 (pp. 1151-1168).

62 Regulamento (UE) n.º 236/2012. do Parlamento Europeu e do Conselho de 14 de março de 2012.

no das "ações *meme*", verificando-se negociação coordenada e para fins distintos dos defendidos pela teoria económico-financeira e pela legislação europeia.

Portanto, o que se espera nos mercados financeiros é que indivíduos e instituições adquiram instrumentos financeiros pelos rendimentos que estes pagam. É este o objetivo com o qual o legislador europeu espera que um investidor razoável negoceie. No entanto, não é o que em grande parte se observa nos acontecimentos descritos, podendo verificar-se distorções destes conceitos e objetivos.

3.1. O OBJETIVO DA REGULAÇÃO DOS MERCADOS FINANCEIROS

Segundo o sublinhado por todos os comités designados pela Comissão Europeia, os principais objetivos da regulação dos mercados financeiros na União Europeia são assegurar a eficiência dos mercados de capitais e a proteção dos investidores[63]. Nos considerandos de diversas diretivas e regulamentos europeus é sublinhada a importância de assegurar o bom funcionamento dos mercados de valores mobiliários e a confiança do público nesses mercados como condição essencial para o crescimento económico e para a prosperidade[64], pois mercados de capitais eficientes promovem o crescimento e a criação de emprego através de uma melhor afetação dos capitais e de uma redução dos custos[65].

O bom funcionamento dos mercados de capitais assenta em três atributos: a eficiência, a liquidez e a estabilidade[66].

a) Eficiência

A conceito de eficiência dos mercados financeiros é composto por quatro dimensões: alocativa, institucional, informativa e operativa.[67]

A eficiência alocativa existe quando o capital de investimento é dirigido através dos preços de mercado para os seus melhores usos possíveis[68], i.e.,

---

63 Christian Bumke, "Regulierung am Beispiel der Kapitalmärkte – Eine Untersuchung über Konzeption und Dogmatik des Regulierungsverwaltungsrechts" in: Klaus Hopt, Rüdiger Veil e Jörn Kämmerer, *Kapitalmarktgesetzgebung im europäischen Binnenmarkt*, 1ª edição, Tübingen, Mohr Siebeck, 2008, p. 118 (pp. 107-142).

64 Considerando 2 do Regulamento (UE) n.º. 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014. Ver também o considerando 3 da DMIF II.

65 Considerando 1 da Diretiva 2004/109/CE do Parlamento Europeu e do Conselho de 15 de dezembro de 2004.

66 Lars Klöhn, "Kapitalmarktrecht" *in* Katja Langenbucher, 4ª edição, *Europäisches Privat- und Wirtschaftsrecht*, Baden-Baden, Nomos, 2017, p. 336.

67 Ibid.

68 Heinz-Dieter Assmann, *Prospekthaftung als Haftung für die Verletzung kapitalmarktbezogener Informationsverkehrspflichten nach deutschem und US-amerikanischem Recht*, Köln, Carl Heymanns Verlag, 1985, p. 25.

para onde este capital é mais necessário e para onde se perspetivam maiores ganhos com menor risco. Para tal, deve ser possível identificar o investimento que maior sucesso promete, o que por sua vez pressupõe que os preços dos instrumentos financeiros têm uma correspondência o mais próxima possível do seu valor fundamental[69].[70] Tal exige preços não só informados, mas também exatos[71]. A eficiência alocativa está diretamente relacionada com a eficiência informativa, mas preços eficientes do ponto de vista da informação não o são necessariamente do ponto de vista da alocação de capital.[72] A eficiência informativa implica apenas que o mercado reage a novas informações de tal forma que os indivíduos não as podem explorar, enquanto que, por sua vez, a eficiência alocativa implica que o mercado reage às novas informações de forma apropriada[73].

A eficiência institucional designa o grau de confiança que os participantes têm no funcionamento do mercado[74]. A confiança dos investidores na integridade e estabilidade do mercado é uma condição essencial para o seu funcionamento, pois estes apenas irão investir as suas poupanças em instrumentos financeiros se acreditarem que os preços são formados de acordo com as leis da procura e da oferta[75].

A existência de eficiência informativa verifica-se quando novas informações são incorporadas nos preços tão rapidamente que os especuladores não podem lucrar apenas com base em tais informações[76]. No entanto é importante sublinhar que a total eficiência informacional é um estado ideal que nunca pode ser plenamente alcançado. Sempre haverá alguém que incorpora a nova informação no preço antes de todos os outros, lucrando com isso e contribuindo para o reajustamento dos preços.[77]

Na teoria económico-financeira, nomeadamente, segundo a chamada forma semi-forte da teoria ECMH, é geralmente assumido que os preços nos mercados de capitais contêm sempre toda a informação conhecida publicamente, ou seja, os investidores só poderiam realizar um lucro acima

---

69 Ver *infra*, Capítulo II 3.

70 Marcel Kahan, "Securities Laws and the Social Costs of Inaccurate Stock Prices", *Duke Law Journal*, Vol. 41, 1992, p. 1006 e ss. (pp. 977-1044). Disponível em: https://scholarship.law.duke.edu/dlj/vol41/iss5/1

71 Lars Klöhn, "Kapitalmarktrecht" *in* Katja Langenbucher, 4ª edição, *Europäisches Privat- und Wirtschaftsrecht*, Baden-Baden, Nomos, 2017, p. 337.

72 Ibid.

73 Ibid.

74 Heinz-Dieter Assmann, *Prospekthaftung als Haftung für die Verletzung kapitalmarktbezogener Informationsverkehrspflichten nach deutschem und US-amerikanischem Recht*, Köln, Carl Heymanns Verlag, 1985, p. 26.

75 Dörte Poelzig, *Kapitalmarktrecht*, 2ª edição, München, C.H. Beck, 2021, p. 13.

76 Ronald Gilson e Reinier Kraakman, "The Mechanisms of Market Efficiency", *Virginia Law Review*, Vol.70, n.º 4, 1984, p. 558 (pp. 549-644)

77 Lars Klöhn, "Kapitalmarktrecht" *in* Katja Langenbucher, 4ª edição, *Europäisches Privat- und Wirtschaftsrecht*, Baden-Baden, Nomos, 2017, p. 337.

da média com base em informação privada não conhecida publicamente.[78] Contudo, esta visão é cada vez mais desafiada sob uma perspetiva teórica e empírica pelas finanças comportamentais[79].

A eficiência operacional prevalece quando os custos de transação nos mercados de capitais são baixos.[80] Quanto menores estes custos, maiores serão os rendimentos dos investidores.[81]

b) Liquidez

A segunda característica dos "bons" mercados de capitais é a liquidez. Os mercados são líquidos quando os investidores podem negociar a qualquer momento em qualquer quantidade, sem a produção de um efeito significativo no preço.[82] A liquidez reduz os custos de transação e conduz a preços mais informativos e precisos, encorajando tanto os investidores de retalho como os investidores profissionais a entrarem no mercado[83]. Os investidores necessitam, assim, de liquidez para negociarem de forma rápida e com os menores custos com outros participantes, encontrando contrapartes para as suas ordens de negociação[84]. Não havendo liquidez, os mercados terão elevados custos de transação implícitos, sendo mais voláteis e menos eficientes[85].

A liquidez é visível olhando ao *bid-ask spread*, o qual espelhará baixos custos de transação em mercados líquidos e elevados custos de transação em mercados ilíquidos[86]. O *bid-ask spread* consiste na diferença entre o preço mais elevado que um comprador está disposto a pagar por um bem (*bid*) e o preço mais baixo que um vendedor está disposto a aceitar (*ask*), correspondendo o *ask* ao preço pelo qual é possível imediatamente comprar e o *bid* ao preço pelo qual é possível imediatamente vender o respetivo título[87].

---

78 Dörte Poelzig, *Kapitalmarktrecht*, 2ª edição, München, C.H. Beck, 2021, p. 18.

79 Dörte Poelzig, *Kapitalmarktrecht*, 2ª edição, München, C.H. Beck, 2021, p. 21.

80 Petra Buck-Heeb*, Kapitalmarktrecht*, 9ª edição, München, C.F. Müller, 2017, p. 3.

81 Dörte Poelzig, *Kapitalmarktrecht*, 2ª edição, München, C.H. Beck, 2021, p. 14.

82 Larry Harris, *Trading & Exchanges*, 1ª edição, Oxford, Oxford University Press, 2002, p. 70.

83 Lars Klöhn, *Kapitalmarkt, Spekulation und Behavioral Finance*, Berlin, Duncker & Hublot, 2006, pp. 68 e ss.

84 Milan Bayram, *Manipulative Handelspraktiken gemäß Art. 12. MAR,* Berlin, Duncker & Hublot, 2020, p. 99.

85 Abdourahmane Sarr e Tonny Lybek, "Measuring Liquidity in Financial Markets", *IMF Working Paper*, 2002, p. 9. Disponível em: https://www.elibrary.imf.org/view/journals/001/2002/232/article-A001-en.xml .

86 Milan Bayram, *Manipulative Handelspraktiken gemäß Art. 12. MAR*, 1ª edição, Berlin, Duncker & Hublot, 2020, p. 101.

87 Zvi Bodie, Alex Kane e Alan Marcus, Investments, 11ª edição, New York, McGraw-Hill Education, 2018, p. 63. John Armour et al., *Principles of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015, p p. 113 e 114.

Por outro lado, o *bid* corresponde à procura e o *ask* à oferta[88]. Por exemplo, se um investidor pretender comprar e imediatamente vender um instrumento financeiro cujos preços de *ask* e *bid* sejam, respetivamente, 10,40 euros e 10,20 euros, irá incorrer num prejuízo de 0,20 euros. Daí, quanto mais líquido o mercado, menor o *spread* e, consequentemente, menores os custos implícitos de transação para os participantes do mercado.

c) Estabilidade

Finalmente, em mercados estáveis os preços só devem flutuar tanto quanto o valor fundamental de um instrumento financeiro varia[89], sendo que qualquer volatilidade para além desta é considerada excessiva. A volatilidade agrada os especuladores, mas afeta a confiança de todos os outros participantes no mercado[90].

3.2. A EFICIÊNCIA DOS MERCADOS E A TEORIA FINANCEIRA NA BASE DA LEI

Se os mercados financeiros fossem perfeitos, estaríamos na presença de eficiência total, o que significaria que os preços nos mercados financeiros espelham o valor fundamental dos seus títulos. Dizendo de outra forma, que os preços dos instrumentos financeiros respondem a toda a informação disponível de forma rápida e eficaz, de forma que os preços reflitam as melhores estimativas possíveis do atual valor económico dos instrumentos financeiros em termos do seus retornos e riscos esperados[91]. Como referido, tal não se verifica.

Na realidade verificam-se assimetrias de informação e relativa falta de transparência. Ainda assim, na batalha contra o abuso de mercado é de grande importância o estado de eficiência de sistemas e informação dos mercados financeiros, pois quanto maior for a eficácia de reflexão de informação relativa ao valor que os preços dos instrumentos financeiros espelham, maior será a dificuldade de perpetração de esquemas abusivos.[92] É neste sentido que o Direito regula os mercados financeiros com o objetivo de obter mercados o mais eficientes possível.

---

88 Ibid.

89 Lars Klöhn, "Kapitalmarktrecht" *in* Katja Langenbucher, 4ª edição, *Europäisches Privat- und Wirtschaftsrecht*, Baden-Baden, Nomos, 2017, p. 338.

90 Larry Harris, *Trading & Exchanges*, 1ª edição, Oxford, Oxford University Press, 2002, p. 316.

91 Lynn Stout, "The Mechanisms of Market Inefficiency: An Introduction to the New Finance", 2003, p. 641, disponível em: https://ssrn.com/abstract=470161

92 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 45.

A teoria da *Efficient Capital Market Hypothesis*[93] (ECMH) de Eugene Fama permanece a teoria de referência quanto à eficiência dos mercados de capitais e a teoria que o Direito dos Valores Mobiliários Europeu segue[94]. Esta teoria contém três formas: forte, semi-forte e fraca.

A forma forte avança que os preços dos instrumentos financeiros refletem com precisão toda a informação relevante sobre um determinado instrumento financeiro, independentemente de a informação ter entrado no domínio público ou permanecer não revelada[95]. Assim, nenhum investidor pode obter retornos em excesso apenas confiando em informações não públicas[96].

A forma semi-forte, pelo contrário, sustenta que os preços dos títulos refletem com exatidão toda a informação disponível ao público e se ajustam instantaneamente e de forma imparcial a novas informações.[97] Assim, nenhum retorno em excesso pode ser ganho com a negociação de informação disponível ao público[98].

A forma fraca sustenta que os preços dos títulos refletem com exatidão apenas informação histórica relativa ao título em particular[99]. Consequentemente, de acordo com esta forma, nenhum retorno em excesso pode ser ganho através da utilização de estratégias de investimento baseadas em preços históricos de ações e outros dados financeiros.[100]

A principal diferença é que sob a forma fraca, um investidor que detém informação privilegiada, sensível aos preços, pode obter ganhos superiores durante um longo período, embora não possa ter um desempenho superior ao do mercado numa base consistente[101]. O mesmo pode acontecer sob a forma semi-forte durante um período mais curto[102]. Tal encoraja os investidores a empenharem-se em estudos do mercado a fim de lucrarem com a informação obtida a título privado através do estudo e análise dos títulos.[103] Os resultados desta pesquisa são comunicados ao mercado sob a forma de informação extraída dos preços a que vários intervenientes no mercado estão dispostos a negociar.[104]

---

93 Eugene Fama, "Efficient Capital Market: A Review of Theory and Empirical Work", The *Journal of Finance*, Vol. 25, n.º 2, 1970, pp. 383-417.

94 Dörte Poelzig, *Kapitalmarktrecht*, 2ª edição, München, C.H. Beck, 2021, p. 23.

95 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 45.

96 Ibid.

97 Ibid.

98 Ibid.

99 Ibid.

100 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 46.

101 Ibid.

102 Ibid.

103 Ibid.

104 Ibid.

Deste modo, e simplificadamente, de acordo com a ECMH um investidor racional procura obter ganhos financeiros, comprando o que é "barato" (subvalorizado) e vendendo o que é "caro" (sobrevalorizado):

> no caso de obtenção de informações positivas, os investidores reagem adquirindo instrumentos financeiros que se encontravam subvalorizados, o que provoca o aumento da procura face à oferta, movendo-se o valor de mercado no sentido do valor fundamental do título, através da sua subida.
>
> no caso de obtenção de informações negativas, os investidores reagem vendendo instrumentos financeiros que se encontravam sobrevalorizados, o que aumenta a pressão do lado da oferta face à procura, movendo-se o valor de mercado no sentido do valor fundamental do título, através da sua descida.

Assim, na realidade, nos mercados de capitais verifica-se (na melhor das hipóteses) a forma semi-forte da teoria ECMH[105], refletindo os preços todas as informações passadas e presentes publicamente conhecidas. Os restantes tipos de mercados financeiros, em particular, de obrigações, mercadorias (*commodities)* e derivados seguem princípios semelhantes[106].

A teoria ECMH tem como uma das suas premissas centrais a de que o investidor negoceia de forma racional utilizando todas as informações essenciais, investindo nos instrumentos financeiros que prometem os maiores rendimentos com menores níveis de risco[107]. No entanto, estudos da área das finanças comportamentais afirmam que os investidores não negoceiam sempre de forma racional[108]. Por exemplo, as bolhas (*bubbles*) são fenómenos causados pela negociação exagerada e não fundamentada de instrumentos financeiros que leva os preços a valores sobrevalorizados e que, como tal, dificilmente podem ser explicados pela teoria da ECMH.[109]

O mesmo podemos verificar no caso da negociação coordenada de pequenos investidores para fins que não a obtenção de ganhos financeiros. Se os investidores de retalho no caso GME pretendessem obter lucro, teriam procedido à venda das ações quando os seus preços estavam (consideravelmente) acima dos valores verificados aquando do início da negociação coordenada. Ao invés, esses investidores não venderam as ações, não obtendo lucro e continuando expostos às acentuadas quedas de preço que mais tarde se viriam a verificar. Muitos deles continuaram a adquirir ações e contratos de opções mesmo em períodos onde os preços se encontravam extremamente sobrevalorizados, expondo-se a riscos ainda

---

105 Ronald Gilson e Reinier Kraakman, "The Mechanisms of Market Efficiency", *Virginia Law Review*, Vol. 70, 1984, p. 551 (pp. 549-644).

106 John Armour et al., *Principles of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015, p. 102.

107 Dörte Poelzig, *Kapitalmarktrecht*, 2ª edição, München, C.H. Beck, 2021, p. 21.

108 Dörte Poelzig, *Kapitalmarktrecht*, 2ª edição, München, C.H. Beck, 2021, pp. 21 e 22.

109 Robert Shiller, *Irrational Exuberance*, 3ª edição, Princeton University Press, 2016, pp. 240 e 241.

maiores, o que confirma a ausência de racionalidade sob o ponto de vista económico-financeiro.

Apesar da evidência, e dos estudos com posições que colocam em causa a teoria ECMH que as finanças comportamentais têm apresentado, não foi ainda apresentada uma melhor alternativa ao nível do Direito, continuando este a trilhar o caminho da otimização das condições nos mercados[110]e de mercados financeiros eficientes[111]. Tal é efetivado através das regras de divulgação de informações relevantes e de proibição dos tipos de abuso de mercado, estando os investidores e participantes dos mercados expostos aos riscos que da normal negociação e natural formação dos preços advêm[112].

É neste âmbito que se afigura extremamente relevante o estudo e discussão do caso GME e das práticas de negociação coordenada entre investidores de retalho através das redes sociais capazes de alterar os preços de forma artificial, afastando-os do seu valor fundamental e contribuindo para a ineficiência dos mercados financeiros.

3.3. O VALOR FUNDAMENTAL E O CAPM

Como referido, a eficiência alocativa pressupõe que os preços dos instrumentos financeiros tenham uma correspondência o mais próxima possível do seu valor fundamental. O valor fundamental é o valor de um instrumento financeiro com o qual todos os intervenientes de mercado concordariam se se encontrassem na posse de todas as informações relevantes[113]. Este deve assim refletir a soma do valor presente dos interesses futuros, ou pagamentos de dividendos, e do preço do instrumento financeiro à data em que o investidor antecipa vendê-lo[114]. Assim, estando os participantes dos mercados financeiros continuamente a atualizar as suas crenças acerca dos lucros futuros em resposta a novas informações, e agregando os preços a que são realizadas as transações nos mercados financeiros informação sobre o valor esperado dos instrumentos financeiros negociados[115], os preços destes devem ser o mais próximo possível dos seus valores fundamentais.

---

110 Ver considerandos 49 e 51 do Regulamento (UE) n.º. 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

111 Dörte Poelzig, *Kapitalmarktrecht*, 2ª edição, München, C.H. Beck, 2021, p. 23.

112 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005.

113 Baruch Lev e Meiring de Villiers, "Stock Price Crashes and 10b-5 Damages: A Legal, Economic, and Policy Analysis", *Stanford Law Review*, Vol. 47, n.º 1, 1994, p. 24 (pp. 7-37).

114 John Armour et al., *Principles of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015, p. 102.

115 John Armour et al., *Principles of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015, p. 101.

Na teoria, da combinação da ECMH com o modelo CAPM (*Capital Asset Pricing Model,* doravante CAPM)[116], o qual assenta nas premissas da primeira, resulta que, num mercado informacionalmente eficiente, os preços refletirão da forma mais próxima possível o valor fundamental dos instrumentos financeiros[117]. O CAPM é um modelo de dois fatores, que descreve a relação quantificável entre risco e retorno esperado para encontrar o valor dos títulos[118]. O rendimento esperado de um título (ou de um portfólio de títulos) é igual à taxa de um título sem risco, acrescida de um prémio de risco multiplicado pelo risco sistemático do ativo[119].

Apesar das críticas que lhe são dirigidas, o CAPM é um dos métodos mais importantes na teoria financeira[120]. Juntando tal ao facto de assentar nas premissas da Efficient Capital Market Hypothesis (doravante ECMH), na qual se baseia o modelo de eficiência que as normas dos mercados de capitais defendem, faz com que o CAPM seja uma solução a ponderar para a investigação da artificialidade do preço[121].

3.4. AS CONSEQUÊNCIAS DA MANIPULAÇÃO DE MERCADO E A NEGOCIAÇÃO COORDENADA NAS REDES SOCIAIS

a) O (inexistente) conceito de manipulação de mercado e a negociação coordenada

Atualmente, não existe uma definição geral e reconhecida do fenómeno económico de manipulação de mercado capaz de descrever de forma razoavelmente concisa os comportamentos abrangidos pelo fenómeno[122]. Tal é visível no artigo 12.º do MAR, no qual o legislador estabelece diferentes tipos de condutas que podem ser classificadas como manipulação de mercado, e infringir a proibição consagrada no art. 15º do MAR.

É relevante trazer aqui a clássica definição do oitavo circuito do Tribunal Federal de Recurso norte-americano (*Federal Court of Appeals*) no caso *Cargill v. Hardin*[123], onde foi estabelecida a definição de manipulação de mercado como um «comportamento que de forma intencional influencie o

---

116 Ver Eugene Fama e Kenneth French, "The Capital Asset Pricing Model: Theory and Evidence", 2003, disponível em: https://ssrn.com/abstract=440920.

117 Lynn Stout, *The Mechanisms of Market Inefficiency: An Introduction to the New Finance*, Cornell Law Faculty Publications, 2003, p. 641, disponível em: https://ssrn.com/abstract=470161.

118 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 52.

119 Ibid.

120 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 53.

121 Ver *infra*, Capítulo IV 1.3.1.

122 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 451.

123 Ver Cargill, Inc v Hardin 452 F 2d 1154, 1164–65 (8th Cir 1971).

preço de mercado de tal maneira que este não mais represente as forças de procura e oferta»[124]. Esta definição clássica inclui fatores que são encarados como constituintes de manipulação, e que são visíveis no caso GME e das "ações *meme*", onde investidores de retalho coordenados através das redes sociais negociaram de acordo com uma estratégia com o objetivo de influenciar os preços, tendo efetivamente conseguido desviar os preços dos seus valores fundamentais[125] e, como tal, do mecanismo de formação dos preços da natural interação entre procura e oferta. A NCIRRS apresenta, em relação às clássicas perceções de manipulação de mercado, a diferença de os efeitos se produzirem apenas através da negociação de todos os participantes de acordo com a estratégia coletiva, pois, considerando a conduta negocial individual de cada participante, não existem fundamentos para esta ser considerada capaz de produzir efeitos como os de uma manipulação de mercado na sua visão mais tradicional.

Tal como afirma Moloney, as práticas manipulativas são uma forma de falha de mercado que pode conduzir a uma ineficiente alocação de recursos e que prejudica o papel do mercado na alocação de capital.[126] É a salvaguarda do regular funcionamento do mecanismo de formação de preços que justifica a incriminação da manipulação de mercado[127].

Tal releva a necessidade de analisar esta prática de negociação coordenada de investidores de retalho através das redes sociais. Antes de tal análise, porém, cabe ponderar as consequências da manipulação de mercado e estabelecer a possível correspondência entre estas e as (possíveis) consequências da referida negociação coordenada.

b) As consequências da manipulação de mercado

Como vimos, para que o bom financiamento dos mercados de capitais seja assegurado, o capital deve ser alocado onde maiores retornos com um melhor nível de risco sejam prometidos, o que leva a que os preços reflitam o valor fundamental das empresas cujos valores mobiliários são negociados, o que, por sua vez conduz a mais baixos custos de transação e menor dificuldade em executar transações, com menores impactos de transação nos preços (menor volatilidade), e a mercados mais estáveis, aumentando também a confiança dos investidores nos mercados financeiros. Neste sen-

---

124 Cargill, Inc v Hardin 452 F 2d 1154, 1164–65 (8th Cir 1971).

125 Neste sentido, a IOSCO afirma que a regulação anti-manipulação se foca em «manter a integridade do preço de mercado dos valores mobiliários, dos contratos derivados e dos instrumentos na base dos contratos derivados.» IOSCO, 2000 IOSCO Market Manipulation Report, n.º 34, p. 8. Disponível em: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD103.pdf (consultado em 21 de junho de 2022).

126 Niamh Moloney, *EU Securities and financial markets regulation*, 3ª edição, Oxford, Oxford University Press, 2016, p. 704

127 Paulo Câmara, *Manual de direito dos valores mobiliários*, 4ª edição, Coimbra, Almedina, 2018, p. 966.

tido, as proibições da manipulação de mercado ambicionam a manutenção da eficiência de mercado e a redução de custos de capital.[128]

As práticas constituintes da manipulação de mercado têm como efeito principal a distorção dos preços nos mercados financeiros, afastando-os dos seus valores fundamentais, i. e. do valor correspondente aos seus lucros futuros. Tal resulta na obtenção de preços artificiais, ou seja, cuja formação não resulta dos mecanismos de procura e oferta. Estas falhas de formação do preço (*mispricing*) nos mercados financeiros repercutem-se na falha dos mercados em refletir, de forma precisa, a informação disponível sobre o valor dos ganhos subjacentes, resultando em má afetação de recursos.[129] A manipulação do mercado prejudica, assim, também a eficiência informativa. Tal pode significar que significativas quantias de investimento serão direcionadas para atividades que os mercados erroneamente identificam como geradoras de elevados retornos, e que pouco investimento será canalizado para aquelas que os mercados subestimam, havendo, por isso, custos económicos reais da má alocação de recursos[130], sendo a eficiência alocativa do mercado perturbada.

A manipulação de mercado prejudica também a confiança que os investidores e os restantes participantes têm no mercado, afetando a eficiência institucional. Se a confiança dos investidores na integridade da formação dos preços desaparecer poderá verificar-se a previsão de George Akerlof do "mercado de limões" (*market for lemons*), verificando-se seleções adversas[131]. Se os investidores desconfiam do mercado, poderão não conseguir distinguir entre bons e maus investimentos. Seguindo Akerlof, em tal situação estes optarão pelos instrumentos financeiros de mais baixo preço (seleção adversa), levando a que os emitentes de instrumentos financeiros de melhor qualidade abandonem o mercado[132]. Finalmente, de acordo com este modelo, o êxodo dos participantes pode levar ao colapso completo de um mercado.[133] Se os investidores abandonarem o mercado devido à perda de confiança, o número de participantes dispostos a negociar irá diminuir, levando a que a liquidez diminua. Tal fará aumentar os custos de negociação implícitos associados ao instrumento de negociação (diminuição da efi-

---

128 Luca Enriques e Matteo Gatti, "Is there a Uniform EU Securities Law After the Financial Services Action Plan?", *Stanford Journal of Law, Business and Finance*, Vol. 14, n.º 1, 2008, p. 43.

129 John Armour et al., *Principles of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015, p.106.

130 Ibid.

131 George Akerlof, "The Market for "Lemons": Quality Uncertainty and the Market Mechanism", *The Quarterly Journal of Economics*, Vol. 84, n.º 2, Oxford, Oxford University Press, 1970, p. 488.

132 Ibid.

133 George Akerlof, "The Market for "Lemons": Quality Uncertainty and the Market Mechanism", *The Quarterly Journal of Economics*, Vol. 84, n.º 2, Oxford, Oxford University Press, 1970, p. 490.

ciência operacional), bem como o *bid-ask spread*.[134] Os mercados podem, assim, tornar-se ilíquidos e, como tal, pouco atrativos para os investidores. Por outro lado, a perda de liquidez corresponderá a um aumento da volatilidade e consequente instabilidade.

O estabelecimento de tais ações concertadas faz perigar também mecanismos como a venda a descoberto. A possibilidade facilitada de um *short squeeze* abriga o perigo de forçar os vendedores a descoberto a saírem do mercado, embora a sua informação, avaliação do mercado e comportamento negocial sejam muito importantes para uma formação eficiente dos preços[135]. Além disso, campanhas como as do caso GME ameaçam os modelos de negócio que consistam na descoberta de empresas cujo preço esteja sobrevalorizado, podendo a venda a descoberto deixar de ser rentável devido ao considerável risco da ocorrência de um *short squeeze* causado por aquisições ou vendas coordenadas de instrumentos financeiros e das potenciais volumosas perdas para os detentores de posições curtas que a eles se associam.[136] O mercado corre assim o risco de perder uma componente essencial no processo de formação de preços eficientes[137] [138], o que é prejudicial para a eficiência a longo prazo. Por sua vez, tal contribuirá para o aumento da volatilidade e do número de títulos sobrevalorizados, o que pode conduzir à formação de bolhas. Por fim, a economia poderá ressentir-se, com dificuldades para as empresas e a diminuição de postos de trabalho.

c) As (possíveis) consequências da negociação coordenada entre investidores de retalho através das redes sociais

À semelhança de uma tradicional prática de manipulação de mercado, a negociação coordenada entre investidores de retalho através das redes sociais tem também potencial para afastar os preços dos instrumentos financeiros dos seus valores fundamentais, resultando numa falha dos preços

---

134 Ver *supra*, Capítulo II 1.2.

135 John Armour et al., *Principles of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015, pp. 195 e 196.

136 Alexander Sajnovits, "GameStop im Lichte der MAR – Meme-Trading, soziale Medien und Handelsbeschränkungen durch Broker", *Zeitschrift für Unternehmens- und Gesellschaftsrecht*, vol. 50, n.º 5, 2021, p. 810 (pp. 804–845).

137 John Armour et al., *Principles of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015, pp. 195 e ss.

138 É importante sublinhar as críticas realizadas às vendas a descoberto devido ao seu perigo especulatório, e que, de facto, estas constituem um perigo real que os legisladores reconhecem e, por isso, regulam com o objetivo de que sejam apenas utilizadas no sentido do apuramento de um preço mais próximo do seu valor fundamental e não no sentido da obtenção de um preço artificial. John Armour et al., *Principles of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015, p. 198. Sobre vendas a descoberto, ver também António Barreto Menezes Cordeiro, Manual de Direito dos Valores Mobiliários, 2ª edição, Coimbra, Almedina, 2019, pp. 210-212.

em refletir a informação disponível sobre o valor dos ganhos subjacentes, e podendo assim levar à falha da alocação de recursos.

No caso GME e das "ações *meme*", a influência da negociação coordenada provocou a sobrevalorização de valores mobiliários de empresas com fracas perspetivas de lucros futuros de acordo com os seus fundamentais, falhando assim os preços em projetar as informações disponíveis acerca das respetivas empresas, prejudicando a eficiência informativa. Tal demonstra o potencial das NCIRRS para afastar os preços dos seus valores fundamentais, falhando estes em espelhar as informações públicas conhecidas, perdendo-se eficiência informativa.

A má alocação de recursos nos mercados financeiros resultante das falhas da eficiência informativa pode também conduzir à maior canalização de capital para investimentos que menores lucros prometem, e a consequente menor alocação para investimentos com melhores perspetivas e potencial. No caso GME e das "ações *meme*" observou-se a alocação de imenso capital em empresas cujos fundamentais ofereciam fraca perspetiva de lucro. Tal espelha a negociação expressiva por motivos de revolta, políticos, sentimentais, nostálgicos, entre outros.[139]

A diminuição da eficiência informativa e alocativa irá também levar à diminuição da confiança dos participantes no mercado, diminuindo a eficiência institucional. No caso GME, o *short squeeze* e o *gamma squeeze* para o qual a negociação coordenada entre investidores de retalho fortemente contribuiu, e que provocou elevados prejuízos a investidores e grandes fundos de investimento (sobretudo aqueles com posições de venda a descoberto), é suscetível de aumentar os receios de que vendas a descoberto sejam alvos para investidores nas redes sociais, que procurem frustrar seus objetivos de quem as realiza. Desta perda de confiança pode resultar a perda de um mecanismo que ajuste preços sobrevalorizados e que previna bolhas[140].

Da diminuição da confiança pode resultar um gradual abandono dos mercados e perda de liquidez, aumentando os custos e gerando instabilidade, à semelhança das consequências da tradicional manipulação de mercado. Os potenciais efeitos negativos da NCIRRS são também reconhecidos pela Reserva Federal americana (*Federal Reserve*), a qual sublinha num dos seus relatórios que a interação dos investidores de retalho nas redes sociais e a sua negociação de "ações *meme*" pode levar a um considerável aumento de volatilidade e eventuais prejuízos para os quais os sistemas de gestão

139 Ver *supra*, Capítulo I 2.2.

140 Muitos economistas, incluindo Robert J. Shiller (laureado com Nobel da Economia em 2013) veem as vendas a descoberto como um importante mecanismo para contrariar o desenvolvimento de bolhas nos mercados financeiros. John Armour et al., *Principles of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015, p. 195.

de risco das instituições financeiras não estão preparados, apresentando, deste modo, riscos para a estabilidade financeira.[141]

Também as bolhas podem ser uma consequência da negociação coordenada entre investidores de retalho através das redes sociais nos casos em que estes tenham como intenção influenciar o preço de um instrumento financeiro no sentido ascendente. Tal cenário verifica-se se o preço ultrapassar o valor fundamental. No caso GME e das ações *meme* podemos afirmar a ocorrência de bolhas, no sentido em que a negociação coordenada provocou uma inflação dos preços de ações de empresas de baixo potencial em relação aos seus respetivos valores fundamentais. A diferença, em comparação com as tradicionais bolhas, será que, no caso da negociação coordenada, os investidores de retalho envolvidos ambicionam a influência do preço. Neste caso, foi neutralizado o mecanismo que poderia ter contribuído para o ajustamento dos preços – as vendas a descoberto – tendo este sido um alvo inicial no caso GME.

Finalmente, da cumulação das consequências referidas pode a economia sofrer com as dificuldades das empresas e a diminuição dos postos de trabalho.

Por conseguinte, verificando-se os números de participantes e a efetiva coordenação necessária entre eles, a NCIRRS tem o potencial para causar impactos semelhantes às consequências da tradicional manipulação de mercado, distinguindo-se desta no sentido em que apresenta a particularidade de, em regra, poder ser realizada apenas por um grande número de participantes coordenados através de publicações nas redes sociais, com um objetivo de influenciar o preço de instrumentos financeiros.

4. A MANIPULAÇÃO DE MERCADO DO MAR

4.1. O REGULAMENTO MAR – MARKET ABUSE REGULATION

Na União Europeia, o regime da manipulação de mercado é estabelecido pelo Regulamento do Abuso de Mercado, o Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014, que estabelece um quadro legal comum aplicável em toda a União Europeia para os propósitos da prevenção e combate do abuso de mercado.[142] O termo "abuso de mercado" é utilizado no regulamento como uma definição genérica que engloba os atos contrários às normas nos mercados financei-

[141] Board of Governors of the Federal Reserve System, Financial Stability Report, novembro de 2021, pp. 18 a 21. Disponível em: https://www.federalreserve.gov/publications/files/financial-stability-report-20211108.pdf (consultado em 09/04/2022).

[142] Elena Guggenberger in Susanne Kalss *et al*., *EU Market Abuse Regulation: A Commentary on Regulation (EU) No 594/2014*, 1ª edição, Cheltenham, Edward Elgar Publishing. 2021, p. 1.

ros, abrangendo os abusos ligados à informação privilegiada e a manipulação de mercado.[143]

No artigo 1.º do MAR, o legislador europeu estabelece o objetivo «de assegurar a integridade dos mercados financeiros na União e promover a confiança dos investidores nesses mercados»[144]. Nesse sentido, a incerteza legal e a arbitragem regulatória devem ser evitadas.[145] Consequentemente, a formal legal de regulamento assegura a aplicação uniforme das normas de abuso de mercado do MAR em todos os Estados-Membros da União Europeia[146], o que aumenta a certeza para todos os participantes do mercado, prevenindo distorções da concorrência e reduzindo custos de *compliance* relativos a atividades transfronteiriças.[147] Os investidores devem poder confiar num preço que evoluiu através da oferta e da procura, e não através da manipulação[148].

O MAR proíbe qualquer pessoa de se envolver em manipulação do mercado[149]. No âmbito pessoal, a proibição da manipulação de mercado aplica-se a todos os participantes do mercado, com especiais condições para o jornalismo[150].

O escopo material do MAR é extenso, sobretudo quando comparado com a anterior Diretiva de Abuso de Mercado de 2003[151].

A principal área de aplicação do MAR é baseada em dois elementos: o instrumento financeiro e o local onde o último pode ser negociado (mercado regulamentado, MTF, OTF). A definição dos instrumentos financeiros e das plataformas de negociação de negociação é realizada na DMIF II.[152]

Quanto aos instrumentos financeiros, estão incluídos todos estes que tenham sido admitidos à negociação em uma das plataformas de negociação, ou para os quais tenha sido efetuado um pedido de admissão à negociação[153].

---

143 Ibid.

144 Artigo 1.º do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

145 Considerando 4 do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

146 Ibid. Em contraste com a diretiva, a qual permite uma relativa discricionariedade dos Estados-membros na implementação das normas, a aplicação imediata e direta do regulamento assegura um quadro legal europeu harmonizado.

147 Considerando 4 do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

148 Lars Teigelack, "Market Manipulation" *in* Rüdiger Veil, *European Capital Markets Law*, 2ª edição, Oxford, Hart Publishing, 2017, p. 227.

149 Artigo 15.º do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

150 ver artigo 21.º do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

151 Niamh Moloney, *EU Securities and financial markets regulation*, 3ª edição, Oxford, Oxford University Press, 2016, p. 740.

152 Artigo 4.º n.º 1 parágrafos 15, 21, 22, 23 e 24 da DMIF II.

153 Niamh Moloney, *EU Securities and financial markets regulation*, 3ª edição, Oxford, Oxford University Press, 2016, pp. 743 e 744.

O MAR aplica-se (i) aos instrumentos financeiros admitidos à negociação num mercado regulamentado ou cuja admissão num mercado regulamentado de um Estado-Membro tenha sido solicitada[154], (ii) aos instrumentos financeiros negociados em sistemas de negociação multilaterais (*Multilateral Trading Facilities,* doravante MTF), admitidos à negociação num MTF ou para os quais tenha sido efetuado um pedido de admissão à negociação num MTF[155], (iii) aos instrumentos financeiros negociados em sistemas de negociação organizados (*Organized Trading Facilities,* doravante OTF)[156] e (iv) aos instrumentos financeiros transacionados em mercado de balcäo (*Over-the-Counter,* doravante OTC) [157] cujo preço ou valor dependa ou tenha efeitos no preço ou valor de um instrumento financeiro do respetivo mercado, como, por exemplo, *swaps* de risco de incumprimento ou contratos diferenciais[158].

Este alargado escopo de aplicação do MAR, cobre, deste modo, instrumentos financeiros que não são diretamente negociados numa plataforma de negociação (mercado regulamentado, MTF ou OTF), mas cujo valor ou preço dependa de um instrumento financeiro negociado ou autorizado em plataformas de negociação. Consequentemente, tentativas de contornar as normas através da utilização de instrumentos financeiros negociados fora

---

154 Artigo 2.º n.º 1 alínea a) do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014. Ver Harry McVea *Supporting Market Integrity in* Niamh Moloney, Eilís Ferran e Jennifer Payne, *The Oxford Handbook of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015, pp. 631 a 658.

155 Artigo 2.º n.º 1 alínea b) do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014. Nos termos do artigo 4.º n.º 1 parágrafo 21 da DMIF II, um mercado regulamentado é «um sistema multilateral, operado e/ou gerido por um operador de mercado, que permite o encontro ou facilita o encontro de múltiplos interesses de compra e venda de instrumentos financeiros manifestados por terceiros – dentro desse sistema e de acordo com as suas regras não discricionárias – por forma a que tal resulte num contrato relativo a instrumentos financeiros admitidos à negociação de acordo com as suas regras e/ou sistemas e que esteja autorizado e funcione de forma regular e nos termos do Título III da presente diretiva;»

156 Artigo 2.º n.º 1 alínea c) do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014. Nos termos do artigo 4.º n.º 1 parágrafo 22, um MTF é um «sistema multilateral, operado por uma empresa de investimento ou um operador de mercado, que permite o confronto de múltiplos interesses de compra e venda de instrumentos financeiros manifestados por terceiros – dentro desse sistema e de acordo com regras não discricionárias – por forma a que tal resulte num contrato nos termos do Título II da presente diretiva»;

157 Artigo 2.º n.º 1 alínea d) do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014. Nos termos do artigo 4.º n.º1 parágrafo 23, um OTF é um «sistema multilateral que não seja um mercado regulamentado nem um MTF dentro do qual múltiplos interesses de compra e venda de obrigações, produtos financeiros estruturados, licenças de emissão ou derivados manifestados por terceiros podem interagir de modo a que tal resulte num contrato nos termos do Título II da presente diretiva»;

158 Elena Guggenberger in Susanne Kalss *et al*., *EU Market Abuse Regulation: A Commentary on Regulation (EU) No 594/2014*, 1ª edição, Cheltenham, Edward Elgar Publishing. 2021, p. 6.

de plataformas de negociação deverão ser prevenidos.[159] Tomando como exemplo os *swaps* de risco de incumprimento e os contratos de diferença referidos na alínea d) do n.º 1 do artigo 2.º, estes são instrumentos financeiros que não são negociados entre partes terceiras através de sistemas multilaterais[160], mas diretamente com o respetivo fornecedor de contratos, v.g., um banco. O MAR aplica-se a todos os instrumentos financeiros cujo preço possa ser derivado direta ou indiretamente de instrumentos das alíneas a) a c) do n.º 1 do artigo 2.º do MAR, independentemente de os primeiros terem ou não admissão a negociação[161]. Outros exemplos de instrumentos financeiros não negociados em plataformas de negociação são os contratos de opções em ações, contratos de derivados em instrumentos financeiros que são negociados fora das plataformas de negociação.

O MAR também se aplica a condutas ou transações, incluindo licitações, relativas à venda em leilão numa plataforma de leilões autorizada como mercado autorizado de licenças de emissão ou de outros produtos leiloados que neles se baseiem, incluindo os casos em que os produtos leiloados não sejam instrumentos financeiros, em conformidade com o Regulamento (UE) n. º 1031/2010[162]. De acordo com este Regulamento, os produtos leiloados são contratos de futuros, produtos a prazo (*forwards*) e produtos à vista de dois dias (*two day spot contracts*)[163].

Em específico, as alíneas a), b) e c) do n.º 2 do artigo 2º do MAR referem apenas a proibição da manipulação de mercado (artigos 12.º e 15.º do MAR) e cobrem apenas os contratos de mercadorias à vista (*spot commodity contracts*), contratos de derivados, outros instrumentos derivados e condutas relativas a índices de referência[164]. Aqui pretendeu o legislador europeu incluir a possibilidade de possíveis efeitos remotos de comportamentos manipulatórios em plataformas de negociação e instrumentos financeiros sob o âmbito do n.º 1 do artigo 2.º do MAR. Os contratos de mercadorias à vista são apenas cobertos sob as condições de não constituírem produtos energéticos grossistas nos termos do Regulamento (UE) 1227/2011 do Parlamento Europeu e do Concelho de 25 de outubro de 2011, e de se tratar de contratos em que a operação, a ordem ou a conduta tem, ou é idónea ou se destina a ter, efeitos no preço ou valor de um instrumento financeiro referido no n.º 1 do artigo 2.º. Os contratos de derivados e outros instrumentos

159 Ibid.

160 Nos termos do artigo 4.º n.º 1 parágrafo 19 da DMIF II, um sistema multilateral é «qualquer sistema ou dispositivo no qual múltiplos interesses de negociação de compra e venda de instrumentos financeiros manifestados por terceiros podem interagir».

161 Elena Guggenberger in Susanne Kalss *et al*., *EU Market Abuse Regulation: A Commentary on Regulation (EU) No 594/2014*, 1ª edição, Cheltenham, Edward Elgar Publishing. 2021, p. 6.

162 Ibid.

163 Artigo 4.º do Regulamento (UE) n.º 1031/2010 da Comissão de 12 de novembro de 2010.

164 Lars Teigelack, "Market Manipulation" *in* Rüdiger Veil, *European Capital Markets Law*, 2ª edição, Oxford, Hart Publishing, 2017, p. 229.

financeiros derivados, por outro lado, são também cobertos pela proibição de manipulação de mercado do MAR, se a operação, a ordem, a oferta ou a conduta tiverem, ou sejam idóneas para ter, efeitos no preço ou valor de um contrato de mercadorias à vista em que o preço ou valor depende do preço ou valor de instrumentos financeiros de acordo com a alínea b) do n.º 2 do artigo 2.º. Tal prende-se com o objetivo de assegurar que também comportamentos manipulatórios indiretos fora do âmbito de aplicação do n.º 1 do artigo 2.º possam ser penalizados.[165] Já a inclusão dos índices de referência (*benchmarks*), tal como definidos no parágrafo 29 do n.º 1 do artigo 3.º do MAR[166], deve-se ao potencial que as manipulações desses índices têm para causar danos duradouros nos mercados financeiros, perceção que foi sobretudo influenciada pelo escândalo LIBOR em 2011[167]. Os índices de referência são usados na determinação de preços e valores de instrumentos financeiros, especialmente de derivados, através da utilização de procedimento pré-estabelecido no que toca à fórmula e à obtenção de dados[168].

O n.º 3 do artigo 2.º do MAR reflete a intenção de abranger a negociação de instrumentos financeiros ao máximo possível[169]. O escopo de aplicação do MAR estende-se a todas as transações, ordens e comportamentos relacionados com qualquer instrumento financeiro referido nos n.ºs 2 e 3 do artigo 2.º do MAR, independentemente de a negociação ter lugar numa plataforma de negociação ou não[170].

O n.º 4 do artigo 2.º do MAR estabelece também a sua aplicação em relação a instrumentos referidos nos n.º 1 e 2 em relação não apenas a comportamentos e omissões na área da União Europeia (doravante UE), mas também em países terceiros[171]. O MAR torna o âmbito de aplicação territorial mais geral, referindo-se única e uniformemente a todo o regime MAR e

---

165 Elena Guggenberger in Susanne Kalss *et al*., *EU Market Abuse Regulation: A Commentary on Regulation (EU) No 594/2014*, 1ª edição, Cheltenham, Edward Elgar Publishing, 2021, p. 8

166 Nos termos do artigo 3.º n.º 1 parágrafo 29 do MAR, índices de referência são «qualquer taxa, índice ou valor divulgado ou publicado que seja, periódica ou regularmente, determinado pela aplicação de uma fórmula ou com base no valor de um ou mais ativos ou preços subjacentes, incluindo preços, taxas de juro ou outros valores reais ou estimados, ou inquéritos por referência aos quais é determinado o montante a pagar ao abrigo de um instrumento financeiro ou o valor de um instrumento financeiro».

167 Elena Guggenberger in Susanne Kalss *et al*., *EU Market Abuse Regulation: A Commentary on Regulation (EU) No 594/2014*, 1ª edição, Cheltenham, Edward Elgar Publishing. 2021, p. 8.

168 Ibid.

169 Considerando 8 do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

170 Elena Guggenberger in Susanne Kalss *et al*., *EU Market Abuse Regulation: A Commentary on Regulation (EU) No 594/2014*, 1ª edição, Cheltenham, Edward Elgar Publishing. 2021, p. 8.

171 Lars Teigelack, "Market Manipulation" *in* Rüdiger Veil, *European Capital Markets Law*, 2ª edição, Oxford, Hart Publishing, 2017, p. 228.

aos instrumentos dos n.º 1 e 2 do artigo 2.º nele abrangidos.[172] A formulação geral utilizada destina-se a assegurar uma proteção abrangente dos mercados de capitais.[173] Neste sentido, salienta-se que todos os casos transfronteiriços a que se referem comportamentos e omissões relacionados com os instrumentos dos n.º 1 e 2 são automaticamente abrangidos pelo âmbito de aplicação do MAR[174]. Por conseguinte, já não será necessário fazer referência a normas de abuso de mercado correspondentes num país terceiro.[175] Eventuais manipulações de mercado realizadas através das redes sociais podem envolver utilizadores localizados em qualquer parte do mundo, o que torna a aplicação do MAR possível, sendo tal suscetível no caso GME.

Com a extensão do seu âmbito material, o legislador europeu pretendeu evitar a arbitragem regulatória entre os locais de negociação e assegurar a proteção do investidor na União Europeia.[176] As atividades monetárias e de gestão da dívida pública e das atividades no âmbito da política para as alterações climáticas estão excluídas do âmbito da regulação.[177]

O MAR utiliza ao longo de todo o regulamento uma cláusula *catch-all,* destinada a captar todas as transações, ordens de negociação ou outras condutas suscetíveis de manipular o mercado, de modo a evitar que possam ocorrer práticas manipuladoras que fiquem fora do seu âmbito[178].

4.2. O REGIME EUROPEU DA MANIPULAÇÃO DE MERCADO

O legislador europeu condensou o conceito de manipulação de mercado no artigo 12.º do MAR.

O MAR estabelece no n.º 1 do artigo 12.º: manipulações à base da negociação, as quais se baseiam na possibilidade de dar sinais falsos ou enganadores em relação à oferta, procura ou preço dos instrumentos financeiros através de ordens de transação[179]; manipulações à base da negociação e da informação, se as transações ou ordens de negociação utilizarem engenhos

---

172 Elena Guggenberger in Susanne Kalss *et al*., *EU Market Abuse Regulation: A Commentary on Regulation (EU) No 594/2014*, 1ª edição, Cheltenham, Edward Elgar Publishing. 2021, p. 8.

173 Elena Guggenberger in Susanne Kalss *et al*., *EU Market Abuse Regulation: A Commentary on Regulation (EU) No 594/2014*, 1ª edição, Cheltenham, Edward Elgar Publishing. 2021, p. 9.

174 Ibid.

175 Ibid.

176 Considerando 8 do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

177 Artigo 6.º do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

178 Niamh Moloney, *EU Securities and financial markets regulation*, 3ª edição, Oxford, Oxford University Press, 2016, p. 717.

179 Artigo 12.º n.º 1 alínea a) do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

fictícios ou outra forma de engano ou artifício[180]; manipulações à base da informação, as quais requerem a disseminação de informações falsas ou enganadoras[181]; e as manipulações de índices (um subtipo de manipulação à base de informação) que ocorrem quando alguém emite uma informação falsa ou enganosa ou um *input* a um índice e sabe ou devia saber que a informação ou *input* eram falsos[182].

No Anexo I do MAR[183], o legislador europeu especifica o significado de manipulações à base de transações e de manipulações através de engenhos fictícios ou qualquer outra forma de engano ou artifício, listando de forma não exaustiva indicadores que devem ser tidos em conta para a investigação de comportamentos que possivelmente se enquadrem à luz do MAR como manipulação de mercado.

O MAR elenca ainda, no n.º 2 do artigo 12.º, outras condutas consideradas como manipulação de mercado, que são concretizações dos tipos estabelecidos no n.º 1[184]. Este elenco é, também, não exaustivo, ou seja, mesmo que nenhuma destas descrições se aplique, uma conduta pode ser considerada como manipuladora de mercado se for enquadrável em alguma das alíneas do n.º 1 do artigo 12.º[185]. Se, pelo contrário, uma destas condutas se aplicar, então há definitivamente manipulação de mercado[186]. Estes exemplos, tratando-se de concretizações dos infrações-base do art. 12.º n.º 1 do MAR, não têm independência deste, pelo que a sua interpretação se realiza em ligação este[187]. O Anexo I do MAR acrescenta, por via do número 3 do artigo 12.º, indicadores não exaustivos que complementam a interpretação das alíneas a) e b) do número 1 do artigo 12.º [188].

No artigo 13.º encontram-se estabelecidas as práticas aceites de mercado (*Accepted Market Practices*), i. e., práticas que poderiam cair no âmbito

---

180 Constitui uma espécie de cláusula de escape, destinada a englobar outros tipos de manipulação de mercado que não os estabelecidos. Artigo 12.º n.º 1 alínea c) do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

181 Artigo 12.º n.º 1 alínea b) do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

182 Artigo 12.º n.º 1 alínea d) do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

183 Anexo I do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

184 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, pp. 585 e 586.

185 Ibid.

186 Lars Teigelack, "Market Manipulation" *in* Rüdiger Veil, *European Capital Markets Law*, 2ª edição, Oxford, Hart Publishing, 2017, p. 231.

187 Ibid.

188 Niamh Moloney, *EU Securities and financial markets regulation*, 3ª edição, Oxford, Oxford University Press, 2016, p. 742.

do artigo 12.º, mas que são excecionalmente aceites por motivos de necessidade, desde que realizadas de acordo com as condições estipuladas[189].

À luz do artigo 15.º do MAR proíbe-se a manipulação de mercado e a sua tentativa, pelo que, por exemplo, uma conduta de manipulação de mercado iniciada, mas, por algum motivo, malsucedida ou não terminada, é também punível.[190] Não é claro qual o momento a partir do qual uma tentativa de manipulação de mercado se inicia[191], mas o considerando 41 do MAR enumera como exemplo de tentativa a situação na qual uma ordem de negociação colocada não é executada devido a razões técnicas. [192]

5. A NEGOCIAÇÃO COORDENADA DOS INVESTIDORES DE RETALHO ATRAVÉS DAS REDES SOCIAIS

A análise deste capítulo incide na efetiva negociação coordenada prosseguida pelos investidores de retalho enquanto coletivo organizado através das redes sociais. Procuraremos analisar o caso GME e das "ações *meme*" à luz da alínea a) do n.º1 e da alínea a) do n.º 2 do artigo 12.º do MAR, tentando ainda avançar com conclusões acerca da NCIRRS.

Os investidores de retalho não têm, individualmente, o poder para influenciarem consideravelmente os preços nos mercados financeiros. No entanto, atualmente, a facilidade de negociação nos mercados financeiros a baixos custos combinada com a interação nas redes sociais, possibilita a coordenação de números imprevisíveis de pequenos investidores de retalho que, facilmente, podem atingir ordens de centenas de milhares, ou até milhões, de investidores. Tal possibilita que pequenos investidores de retalho em negociação coordenada possam ter no mercado o peso de um grande investidor institucional[193], realizando cada investidor de retalho atos negociais de acordo com a estratégia coletiva. Tal pode colidir com os objetivos expressos no art. 1.º do MAR de «assegurar a integridade dos mercados financeiros na União e promover a confiança dos investidores nesses mercados»[194].

---

189 Niamh Moloney, *EU Securities and financial markets regulation*, 3ª edição, Oxford, Oxford University Press, 2016, p. 750.

190 Lars Teigelack, "Market Manipulation" *in* Rüdiger Veil, *European Capital Markets Law*, 2ª edição, Oxford, Hart Publishing, 2017, p. 231.

191 Marc Ventoruzzo e Sebastian Mock, *Market Abuse Regulation Commentary and Annotated Guide*, 1ª edição, Oxford, Oxford University Press, 2017, p. 333.

192 Considerando 41 do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

193 Franklin Allen *et al*., "Squeezing Shorts Through Social Media Platforms", *Swiss Finance Institute Paper n.º 21-31*, 2021, p. 35, disponível em: https://ssrn.com/abstract=3823151

194 Artigo 1.º do Regulamento (UE) n.º. 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

5.1. ART. 12.º N.º 1 ALÍNEA A) DO MAR

O art. 12.º n.º 1 alínea a) do MAR estabelece que constituem atividades de manipulação de mercado a realização de operações, colocação de ordens ou qualquer outra conduta, que sejam idóneas[195] a dar indicações falsas ou enganosas relativamente à oferta, procura ou preço de um instrumento financeiro (alínea a) i); ou que sejam idóneas a fixar os preços dos últimos em valores anormais ou artificiais (alínea a) ii). Preenchendo-se tais requisitos, uma conduta só não será manipulatória se preencher os requisitos estabelecidos no art. 13.º do MAR para ser considerada como prática de mercado aceite.

O artigo 12.º n.º 1 alínea a) do MAR é, por aplicação do art. 12.º n.º 3 do MAR, complementado pelos indicadores do Anexo I Secção A, os quais, por sua vez, concretizando o art. 12.º n.º 5 do MAR, são complementados pela Comissão no Anexo II Secção 1 do Regulamento Delegado 2016/522, por via do art. 4º n.º 1 do mesmo regulamento delegado, onde são fornecidos exemplos de práticas e indicadores adicionais.

a) Operações, a colocação de uma ordem ou outras condutas

As infrações estabelecidas na referida alínea abrangem operações, a colocação de ordens ou outras condutas. Consideram-se como "operações" quaisquer atos negociais de transação independentemente de qualquer mudança de propriedade do instrumento, englobando assim não apenas as compras e vendas de instrumentos financeiros, mas também as promessas[196]. Além do mais, da interpretação da alínea c) da secção A do anexo I do MAR retira-se que também são abrangidos pela norma os negócios fictícios, e não apenas negócios válidos com efeitos económicos[197].

A colocação de uma ordem corresponde ao termo de ordem no sentido negocial, não sendo relevante se se trata de uma ordem de compra ou de venda. Apenas releva a colocação da ordem, pelo que ordens de negociação que não sejam preenchidas, ou sejam submetidas sem intenção, são também abrangidas pelo artigo[198].

Já com a expressão "outras condutas", o legislador procura alargar ao máximo o escopo de condutas que podem ser abrangidas pela alínea a), incluindo até as formas próprias da manipulação através de informação[199].

---

195 Termos da versão portuguesa do MAR. Ver nota de rodapé 200.

196 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 524.

197 «A realização de operações sem alterações nos beneficiários económicos de um instrumento financeiro, contrato de mercadorias à vista com ele relacionado ou produto leiloado com base nas licenças de emissão;», Anexo I Secção A do Regulamento (EU) n.º 596/2014 do Parlamento Europeu e do Conselho.

198 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 525.

199 Ibid.

No caso GME e das "ações *meme*", verificamos que, em resultado da discussão e instruções nas redes sociais, os investidores de retalho consumaram esta estratégia através da negociação individual coordenada de instrumentos financeiros de acordo com a estratégia coletiva definida nas redes sociais.

Deste modo, a nosso ver, podem ser inseridos no âmbito da referida alínea não só os comportamentos negociais (a concreta negociação), mas também as publicações nas redes sociais parte da articulação dos investidores de retalho para a negociação coordenada (nas quais incidirá o foco do capítulo seguinte).

b) Adequação para dar indicações falsas ou enganosas

Nos termos do art. 12.º n.º 1 alínea a) i) do MAR, verifica-se uma manipulação de mercado se uma conduta negocial é, provavelmente[200], adequada para dar indicações falsas ou enganosas, relativamente à oferta, procura ou preço de um instrumento financeiro.

No sentido da referida alínea, estamos perante «indicações» quando de uma determinada conduta negocial um investidor razoável pode, no âmbito da sua tomada de decisão de investimento, pelo menos provavelmente, tomar em consideração qualquer informação acerca da oferta, procura ou preço de um instrumento financeiro.[201]

É relevante destacar que a conduta negocial não se resume à venda ou compra de instrumentos financeiros, pelo que a manutenção de um instrumento financeiro é também suscetível de ser interpretada pelos investido-

[200] Na versão portuguesa do MAR, é utilizada a expressão «dê ou seja idónea para dar», sendo imposta uma condição mínima de idoneidade pelo legislador. Já na versão alemã o legislador refere-se concretamente à probabilidade («*gibt oder bei der dies wahrscheinlich ist*», que significa "dá ou provavelmente dá"), o que implica um maior grau de probabilidade, quando comparado com a versão portuguesa do regulamento. É importante perceber exatamente qual a exigência de probabilidade. Ora, para a interpretação do Direito da União Europeia e, como tal, também do MAR há uma igualdade entre todas as versões nas diferentes línguas, mas, como é evidente, não se irá na prática comparar todas as versões linguísticas do regulamento. No entanto, tendo a versão original do MAR sido realizada e discutida em língua inglesa, afigura-se, em caso de dúvida de interpretação, mais relevante olhar a esta versão. Nesta, a expressão utilizada é «*gives, or is likely to give*» o que indica um maior grau de probabilidade, indo assim no sentido da expressão de probabilidade utilizada na versão alemã. É também este o sentido que aqui seguimos. Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, pp. 477, 478 e 523. Rüdiger Veil, "Europäisches Insiderrecht 2.0 – Konzeption und Grundsatzfragen der Reform durch MAR und CRIM-MAD", *Zeitschrift für Bankrecht und Bankwirtschaft*, 2014, p. 88.

[201] Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 526.

res, produzindo efeitos[202]. Quanto ao grau da referida probabilidade, o mesmo não foi especificado pelo legislador europeu[203].

A adequação de um determinado comportamento negocial para a produção de efeitos dos quais investidores razoáveis possam retirar indicações não pode ser generalizada, i.e., um comportamento negocial pode ser adequado a produzir efeitos num tipo de mercado, mas não o ser num outro mercado diferente[204]. Concretizando: uma ordem de compra ou venda de um determinado instrumento financeiro produzirá maiores efeitos de informação num mercado de menor liquidez do que num mercado de maior liquidez. Assim, v.g., uma ordem negocial de compra ou venda de 100 ações no mercado regulamentado português (bolsa de Lisboa) pode constituir uma indicação, produzindo efeitos informacionais para um investidor razoável. Pelo contrário, uma ordem negocial de compra ou venda de 100 ações de uma empresa constituinte do índex *S&P 500* não constituirá uma indicação, visto que não produz qualquer tipo de informação a ser considerada pelo investidor razoável. Por conseguinte, é necessária uma análise do caso concreto para a determinar se uma determinada conduta negocial pode constituir uma indicação para um investidor razoável[205].

A interpretação segundo a perspetiva de investidor razoável é o critério de interpretação de referência do Direito dos Valores Mobiliários Europeu. Um investidor razoável é um investidor adequadamente informado, atento, com espírito crítico e familiarizado com as dinâmicas e acontecimentos dos mercados financeiros[206]. Este tem também em consideração as reações irracionais de outros investidores na medida em que estas constituam irracionalidades previsíveis[207]. Segundo o considerando 14 do MAR, o investidor razoável baseia-se, para a tomada de decisões de investimento, nas informações colocadas *ex ante* à sua disposição[208].

---

202 Por exemplo, se uma empresa divulga resultados financeiros abaixo do previsto é de esperar que um investidor razoável atualize a sua avaliação da empresa, vendendo as ações, contribuindo para um ajustamento do preço. Se perante tal cenário, o investidor razoável não vende, tal irá dar indicação ao mercado de que, apesar dos resultados financeiros abaixo do esperado, a empresa poderá ter ainda valor.

203 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 527.

204 Milan Bayram, *Manipulative Handelspraktiken gemäß Art. 12. MAR*, 1ª edição, Berlin, Duncker & Hublot, 2020, p. 57.

205 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 527.

206 Ibid.

207 Ibid.

208 «Os investidores razoáveis baseiam as suas decisões de investimento nas informações colocadas à sua disposição, isto é, informações disponíveis ex ante. Por conseguinte, a questão de saber se um investidor razoável, ao tomar a sua decisão de investimento é suscetível de ter em conta uma dada informação, deverá ser apreciada com base na informação disponível ex ante. Esta avaliação deve ter em conta o impacto previsível das informações, à luz do conjunto das atividades do emitente com elas relacionadas, a fiabilidade da fonte

No caso GME e das "ações *meme*", a negociação coordenada através das redes sociais por investidores de retalho constitui a conduta. Esta conduta, na medida em que introduziu grandes alterações nos preços de ações de empresas[209], produziu efeitos sob a forma de informação que um investidor razoável, provavelmente, interpretaria. Consequentemente, a conduta de negociação coordenada nas redes sociais por investidores de retalho é suscetível de dar indicações aos restantes investidores, visto que produz efeitos sob a forma de informação que, pelo menos provavelmente, será interpretada por um investidor razoável.

Para a aplicação do art. 12.º n.º 1 alínea a) i) do MAR, não chega que uma conduta negocial possa ser considerada como apta a dar uma indicação. O legislador europeu especifica que a indicação deve ser falsa ou enganosa.

Segundo Schmolke, uma indicação é falsa se contrariar a verdadeira situação de mercado do respetivo instrumento financeiro a que se refere; e enganosa se for suscetível de criar, em relação ao respetivo instrumento financeiro a que se refere, perceções erradas[210] a um investidor razoável[211].

Acrescenta-se que a avaliação do carácter de uma indicação é uma tarefa complexa, pelo que deve ter por base uma análise *ex post* objetiva de um especialista[212].

Tendo já analisado a conduta de NCIRRS enquanto conduta suscetível de dar indicações aos restantes investidores, segue-se a análise do carácter das mesmas indicações. A negociação coordenada nas redes sociais contribuiu nos casos GME e das "ações *meme*" para elevar os cursos das ações da GME e de outras empresas[213] para níveis considerados por especialistas como sendo sobrevalorizados, uma vez que os preços não correspondiam ao valor fundamental das ações das respetivas empresas. Para além disso, podem induzir os restantes investidores em erro em relação ao preço e procura dos instrumentos financeiros na medida em que representam algo

de informação e quaisquer outras variáveis do mercado que, nas circunstâncias em causa, possam afetar os instrumentos financeiros, os contratos de mercadorias à vista com eles relacionados ou os produtos leiloados com base nas licenças de emissão.» Considerando 14 do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho.

209 No caso GME e das ações meme, estamos perante ações listadas em mercados regulamentados norte-americanos de grande liquidez, onde seria mais difícil, devido à quantidade de capital necessário, obter uma produção de efeitos suscetíveis de serem interpretados por um investidor razoável.

210 As indicações falsas na medida em que retratam uma situação que não se verifica, criam também perceções erradas a um investidor razoável. Neste sentido, o conceito de indicação enganosa inclui, já em si, o conceito de indicação falsa. Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 528.

211 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 528.

212 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 529.

213 Ver *supra*, Capítulo I.

que não corresponde à verdade. Por conseguinte, a nosso ver, a negociação coordenada nas redes sociais por investidores de retalho pode, conforme o caso concreto, provavelmente dar indicações falsas ou enganosas no que respeita à oferta, procura e preço de instrumentos financeiros.

No entanto, se as transações se concentrarem num determinado momento ou período de tempo, tal envia sinais completamente diferentes ao mercado, quando comparado com a colocação de transações não coordenadas espalhadas por um horizonte temporal mais largo, inclusivamente em termos de volume[214].

Como verificado no caso GME e das "ações *meme*" (e como se assume numa NCIRRS que atinja efeitos relevantes) a negociação coordenada verifica-se num espaço temporal relativamente concentrado, sendo provável que provoquem oscilações suficientemente relevantes dos preços para que sejam consideradas por um investidor razoável enquanto potencialmente transmissoras de uma indicação em relação ao instrumento financeiro. Mas deverá sempre analisar-se o caso concreto, pois se não forem provocadas oscilações suficientemente consideráveis do preço, então estas não serão tidas em conta por um investidor razoável[215].

Assim, se numerosas ordens de negociação são colocadas no mercado por um grande número de pessoas de forma concertada num determinado momento, tal implica para o investidor razoável a existência de novas informações relevantes em termos de preço para o respetivo instrumento financeiro ou para o seu emitente, o que também o pode induzir a tomar uma decisão de investimento[216]. Uma vez que, no âmbito da negociação coordenada, tais informações relativas ao preço de um instrumento ou ao seu emitente na realidade não existem, a negociação coordenada será adequada para enviar uma indicação enganosa[217].

---

214 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 529.

215 No caso GME, o aumento dos preços das ações atingiu valores percentuais superiores a 1000%, algo que nenhum investidor poderia ignorar. Ver *supra*, Capítulo I 1.2.

216 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 529. Franklin Allen e Douglas Gale apresentaram um modelo segundo o qual os comportamentos negociais de determinados grandes investidores emitem sinais ao mercado, os quais são interpretados por certos investidores (investidores de informação) como negociação devido a novas informações, as quais podem nem sequer existir. A concentração temporal de uma multiplicidade de pequenas ordens pode criar um efeito semelhante. Franklin Allen e Douglas Gale, "Stock-Price Manipulation", *Review of Financial Studies*, Vol. 5, n.º 3, 1992, p. 503 (pp. 503-529).

217 Alexander Sajnovits, "GameStop im Lichte der MAR – Meme-Trading, soziale Medien und Handelsbeschränkungen durch Broker", *Zeitschrift für Unternehmens- und Gesellschaftsrecht*, vol. 50, n.º 5, 2021, p. 819 (pp. 804–845).

c) (Provável) criação de um nível de preços anormal ou artificial

O art. 12.º n.º 1 alínea a) ii) do MAR estabelece, como requisito para inserção no escopo da manipulação de mercado, que uma conduta produza, ou provavelmente[218] produza, um nível de preços anormal ou artificial. Do enunciado podemos retirar que o legislador europeu não estabelece que os preços se devem tornar anormais ou artificiais, bastando que tal efeito seja de esperar[219].

Quanto à idoneidade para assegurar preços artificiais, basta uma influência no preço de curto espaço temporal. Tal foi definido pela jurisprudência do Tribunal de Justiça da União Europeia (doravante TJUE) no caso IMC *Securities* ao estabelecer que os objetivos prosseguidos «ficariam comprometidos se comportamentos pudessem eximir-se à proibição de manipulação de mercado pelo simples facto de terem dado lugar a uma única transação e, consequentemente, a uma única cotação, sem que o preço do instrumento ou dos instrumentos financeiros em causa mantivesse um nível anormal ou artificial para lá de um certo período.»[220]. O TJUE justificou tal com o objetivo da proibição da manipulação de mercado, uma vez que a confiança na integridade dos mercados financeiros já pode ser afetada pela criação a curto prazo de um nível de preços artificial[221].

Importa seguidamente perceber, portanto, o que significa um preço artificial ou anormal, sendo que tal não é definido pelo legislador europeu. A International Organization of Securities Commissions (doravante IOSCO)[222] define a artificialidade dos preços como «o desvio dos preços em relação às legítimas forças da oferta e da procura».[223] No entanto, aqui também é deixada em aberto a questão acerca de quando um desvio do preço constituirá um legítimo comportamento de mercado, como parte da interação das forças de procura e oferta[224].

---

218 Ver nota de rodapé 200.

219 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 530.

220 TJUE, 7.7.2011, Processo C-445/09 – (IMC Securities), ECLI:EU:C:2011:459, disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0445

221 Ibid.

222 A *International Organization of Securities Commissions* (IOSCO) é o organismo internacional que reúne os reguladores de mercados de capitais do mundo e é reconhecido como o organismo que estabelece os padrões da regulação de valores mobiliários. A IOSCO desenvolve, implementa e promove a adesão a normas internacionalmente reconhecidas para a regulamentação de valores mobiliários. Ver https://www.iosco.org/about/?subsection=about_iosco

223 IOSCO, Investigating and Prosecuting Market Manipulation, maio de 2000, p. 13. «Price artificiality is the divergence of price from the legitimate forces of supply and demand. In order to establish price artificiality, it is therefore necessary to accumulate evidence that prices did not follow legitimate economic forces.». Disponível em: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD103.pdf

224 Daniel Fischel e David Ross, "Should Law Prohibit Manipulation?", Harvard Law Review, Vol. 105, 1991, pp. 508 e 509 (pp. 503-553).

A nosso ver, olhando aos objetivos da regulação dos mercados financeiros, um preço artificial será um preço que se afaste do valor fundamental de um instrumento financeiro, o que tem graves implicações para a eficiência, liquidez, volatilidade e estabilidade dos mercados financeiros.

Para responder a esta questão, são conhecidas as seguintes possibilidades: o teste da perspetiva histórica (*historical approach*), o teste do preço não usual (*unusual price test*) e a utilização de estudo de casos.

No teste da perspetiva histórica, o hipotético desenvolvimento dos cursos na ausência de comportamentos manipulativos é calculado recorrendo aos dados históricos e comparado com os efetivos preços de mercado[225].

A perspetiva histórica apresenta a limitação de não poder ser aplicada em instrumentos financeiros que só recentemente (em relação à data da análise) iniciaram a sua negociação nos mercados financeiros, visto que não haverão dados históricos para a realização da análise, tal como se verifica, p. e., no caso de uma oferta inicial.[226] Além disso, será difícil apurar a atual procura e oferta de um instrumento financeiro com base na procura e oferta passada, já que os dados históricos não incorporam informação sobre acontecimentos inéditos[227] ou a procura de novos tipos de investidores e requisitos de origem diversa, os quais por sua vez refletem as expectativas sobre o futuro nível dos preços dos instrumentos financeiros[228].

No teste do preço não usual procuram identificar-se desenvolvimentos de preços não comuns e inexplicáveis, os quais constituirão um indício da artificialidade dos preços[229]. Tal aplica-se, por exemplo, no caso da existência de discrepâncias não comuns entre os desenvolvimentos dos preços de ações e de instrumentos financeiros derivados com base nas primeiras[230]. Este teste pode padecer do facto de os preços com os quais são realizadas as comparações poderem, eles próprios, ser influenciados por atividade manipulativa[231]. Por outro lado, não apenas a manipulação de mercado pode causar anomalias no desenvolvimento dos preços[232], podendo estas tam-

---

225 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, pp. 109 e 110.

226 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 110.

227 tal como o impacto das redes sociais na negociação nos mercados financeiros na atualidade.

228 Wendy Perdue, 'Manipulation of Futures Markets: Redefining the Offense', *Fordham Law Review*, Vol. 56, n.º3, 1987, p. 377 e 378 (pp. 345-402).

229 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 111.

230 Ibid.

231 Ibid.

232 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 111.

bém ser causadas pelo impacto de declarações incorretas ou outras formas de desinformação[233].

Assim, a perspetiva histórica e o teste dos preços não usuais não fornecem, diretamente, uma solução válida para a avaliação da probabilidade de produção de efeitos manipulativos sobre os preços[234], bem como nos casos de manutenção de um preço artificial ou de uma tentativa de manipulação[235].

Por último, surge a utilização de casos de estudo. Utilizando este método, primeiro identifica-se o evento causador da possível distorção no mercado e o período de tempo no qual a conduta influenciou ou continuou a influenciar o preço de mercado (janela de tempo). No seguimento deste processo, um modelo como o modelo CAPM (*Capital Asset Pricing Model*)[236] é utilizado para identificar o normal comportamento dos instrumentos financeiros[237].

Neste processo, especialistas determinam se o evento, enquanto nova informação, afeta o preço do valor mobiliário, examinando se, para o período em que evento se verifica, os preços verificados seriam diferentes dos preços que se obteriam num desenvolvimento de mercado sem a ocorrência do evento.[238]

Assim, um estudo de caso consiste numa comparação do nível de preços real com um hipotético desenvolvimento de preços sem manipulação - ou seja, um desenvolvimento de preços quando o comportamento potencialmente manipulador é desconsiderado[239]. Desta forma o nível do preço que se verificaria se a negociação coordenada não tivesse interferido só pode ser determinado com recurso aos resultados dos estudos do mercado de capitais[240].

No âmbito da NCIRRS, o estudo de caso deve, a nosso ver, também ser complementado pela investigação realizada por empresas especializadas

---

233 Richard Friedman, "Stalking The Squeeze: Understanding Commodities Market Manipulation", *Michigan Law Review*, Vol. 89, 1990, p. 56 (pp. 30-68).

234 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 531.

235 Ibid.

236 O modelo a aplicar pode variar de acordo com o instrumento financeiro em questão. Por exemplo, o CAPM terá aplicação em valores mobiliários, enquanto para a determinação de preços de opções se aplica o modelo de Black-Scholes. Ver Zvi Bodie, Alex Kane e Alan Marcus, Investments, 11ª edição, New York, McGraw-Hill Education, 2018, pp.714 e ss.

237 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 493.

238 Jonathan macey *et al*., "Lessons from Financial Economics: Materiality, Reliance, and Extending the Reach of Basic v. Levinson", *Virginia Law Review,* Vol. 77, 1991, p. 1029 (pp. 1017-1049). Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 493.

239 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 493.

240 Peter Mülbert, "Art. 12. VO Nr. 596/2014", in: Heinz-Dieter Assmann, Uwe Schneider e Peter Mülbert, *Wertpapierhandelsrecht*, 7ª edição, Köln, Otto Schmidt, 2019, parágrafo 68.

em acompanhar e analisar as publicações que ocorrem nas redes sociais[241]. Assim, mediante as movimentações dos preços (especialmente oscilações sem razão de ordem fundamental) pode ser analisada mais pormenorizadamente a atividade nas redes sociais, de modo a detetar movimentos de concertação para NCIRRS que possam ter influenciado os preços[242].

A vantagem deste método do estudo de caso é que permite a tomada em consideração de padrões de desenvolvimento do preço. Além disso, a utilização de métodos desenvolvidos pela teoria financeira e que emanam da ECMH, como o modelo CAPM, mostra-se em linha com a perspetiva de eficiência seguida pelo Direito[243]. Através do CAPM obtém-se indicadores acerca da eficiência de um mercado uma vez que, num mercado eficiente, a taxa de rendimento de instrumentos financeiros de igual risco não deve ser diferente[244]. No entanto cabe, por outro lado, ressalvar que podem ocorrer desvios devido a falhas no modelo[245].

Por outro, lado é difícil a definição do concreto evento em análise, bem como do espaço temporal da sua atuação[246]. Este espaço temporal deve ser curto o suficiente para excluir a manifestação de outras informações, e largo o suficiente para incluir toda a informação relevante[247], havendo, por isso, o risco de contágio da janela temporal por eventos não relacionados[248].

A nosso ver, o facto de os estudos de caso utilizarem apenas os preços constituirá uma desvantagem. A realização do estudo de casos deve envolver também indicadores como a liquidez, os volumes de transação ou a volatilidade de mercado[249], uma vez que estes são elementos nos quais

---

241 Tal é o caso da empresa *Stockpulse* que trabalha em conjunto com os departamentos de supervisão de negociação das entidades gestoras de mercados Nasdaq e Deutsche Börse. Antonia Mannweiler, "Hashtag #Marktmanipulation", Frankfurter Allgemeine Zeitung, outubro de 2021, disponível em: https://www.faz.net/aktuell/finanzen/aktienmarkt-und-social-media-verdacht-auf-marktmanipulation-17570647.html (consultado a 06/06/2022).

242 Ver Antonia Mannweiler, "Hashtag #Marktmanipulation", Frankfurter Allgemeine Zeitung, disponível em: https://www.faz.net/aktuell/finanzen/aktienmarkt-und-social-media-verdacht-auf-marktmanipulation-17570647.html (consultado a 06/06/2022).

243 Ver *supra*, Capítulo II 2.

244 Milan Bayram, Manipulative Handelspraktiken gemäß Art. 12. MAR, 1ª edição, Berlin, Duncker & Hublot, 2020, p. 98.

245 Milan Bayram, Manipulative Handelspraktiken gemäß Art. 12. MAR, 1ª edição, Berlin, Duncker & Hublot, 2020, p. 99.

246 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 493.

247 Lawrence Cunningham, "Capital Market Theory, Mandatory Disclosure and Price Discovery", Washington and Lee Law Review, Vol. 51, n.º 3, 1994, pp. 850 e 851 (pp. 843-877).

248 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 493.

249 Ver *supra*, Capítulo II. Ver também Milan Bayram, Manipulative Handelspraktiken gemäß Art. 12. MAR, 1ª edição, Berlin, Duncker & Hublot, 2020, pp. 98 a 111.

assenta o bom funcionamento dos mercados financeiros, essenciais à integridade dos mercados[250].

Nos casos GME e das "ações *meme*", a criação de um nível de preços que se desvie do preço que se verificaria sem a intervenção dos investidores de retalho através das redes sociais dificilmente pode ser posta em causa, pelo menos na medida em que o comportamento dos investidores de retalho que comunicam nas redes sociais, exibindo uma certa concertação, e o consequente "encurralamento" de vendedores a descoberto tem um efeito de preço tão significativo.[251] É nesse sentido que apontam os diversos estudos que aqui têm sido mencionados[252]. Dos vários estudos[253] de caso de especialistas se interpreta a influência da NCIRRS nos preços, desviando-os do respetivo valor fundamental e adulterando, assim, os mecanismos de formação de preço.

No caso GME podem ser abrangidos dois indicadores do Anexo II do Regulamento Delegado 2016/522. Os investidores de retalho através da aquisição de ações e derivados de opções das ações da GME negociaram dois instrumentos financeiros conexos. Como referido *supra*, as aquisições de contratos de opções e das ações base dos contratos derivados provocaram um aumento considerável do preço das ações da GME. Os investidores de retalho influenciaram, deste modo, indevidamente o preço de um instrumento financeiro conexo noutra plataforma de negociação, tal como na aceção da manipulação entre produtos do indicador da alínea d) do n.º 2 da Secção 1 do Anexo II do Regulamento Delegado 2016/522.

Por outro lado, da NCIRRS no caso GME resultou uma influência significativa que distorceu substancialmente os preços a que os fundos de investimento de alto retorno com posições a descoberto tinham de entregar as ações a fim de satisfazerem as obrigações resultantes das vendas a descoberto. Deste modo também o indicador da alínea b) do n.º 2 da Secção 1 do Anexo II do Regulamento Delegado 2016/522 pode, parcialmente, encontrar aplicação.

É ainda relevante considerar que a obtenção de efeitos nos preços é também mais fácil de ser obtida em mercados menos líquidos, visto que será menor a quantidade de capital necessária para mover os preços. Tal atribui ainda mais relevo ao caso GME visto que através da NCIRRS foi atingida

---

250 Ver *supra*, Capítulo II.

251 Alexander Sajnovits, "GameStop im Lichte der MAR – Meme-Trading, soziale Medien und Handelsbeschränkungen durch Broker*", Zeitschrift für Unternehmens- und Gesellschaftsrecht*, vol. 50, n.º 5, 2021, p. 820 (pp. 804–845).

252 Ver Joshua Mitts *et al.*, "A Report by the Ad Hoc Academic Committee on Equity and Options Market Structure Conditions in Early 2021", 2022, disponível em: https://ssrn.com/abstract=4030179 . Franklin Allen *et al.*, "Squeezing Shorts Through Social Media Platforms", *Swiss Finance Institute Research Paper No. 21-31*, 2021, disponível em: https://ssrn.com/abstract=3823151, p. 35. Ver também *supra*, Capítulo I.

253 Ibid.

uma influência bastante elevada[254] no mercado de capitais mais líquido do mundo, e, como tal, no mercado onde, à partida, mais difícil seria obter uma influência de tão grande ordem nos preços. Daqui se retira que uma prática de NCIRRS com muitos participantes pode, no mínimo, provavelmente, afastar o preço de um instrumento financeiro do seu valor fundamental. No entanto, sublinha-se esta avaliação é mais eficaz se for realizada *ex post,* no sentido de uma verificação da influência da estratégia coordenada nos preços.

d) O problema da intenção e dos motivos

Um importante ponto, que nos cumpre analisar dada a sua relevância, é o referente à ponderação da intenção e dos motivos no âmbito do art. 12.º n.º 1 alínea a) i) do MAR.

Claramente, o legislador europeu não pretendeu acrescentar requisitos subjetivos relativos às intenções e motivos ao delito de manipulação de mercado[255]. A este respeito, a ESMA afirmou já também que mesmo práticas realizadas sem intenção serão consideradas para a aplicação do artigo 12.º do MAR[256].

É certo que nenhum investidor é obrigado a negociar de forma racional sob um ponto de vista económico-financeiro. No entanto, a posição adotada pelo Direito parte do princípio de que um investidor razoável investe com vista a obter lucros máximos para um certo nível de risco. É também o que se verifica (pelo menos maioritariamente) na realidade, caso contrário, os mercados financeiros perderiam a sua função de, por um lado, financiar empresas e atividades económicas e, por outro lado, de proporcionar rendimentos aos investidores.

Os casos GME e das "ações *meme*" demonstram, a este propósito, a negociação por motivos outros que não a maximização de lucros e a variabilidade das intenções e motivos por detrás de uma estratégia de NCIRRS. As redes sociais permitem a obtenção de um número tão elevado de participantes que será possível que se verifiquem consequências visíveis da negociação não racional, ao contrário do que aconteceria se apenas investidores de retalho negociassem individualmente e de forma economicamente não racional.

No caso GME, o motivo principal que levou à negociação coordenada foi o objetivo de fazer frente aos grandes fundos de investimento de alto retorno. Por outro lado, em parte no caso GME e com maior predominância nas "ações *meme*", manifestam-se os motivos diversos que expressam emoções e sentimentos. Há aqui um claro objetivo de influenciar os preços. É uma ne-

---

254 Ver *supra*, Capítulo I.

255 Milan Bayram, Manipulative Handelspraktiken gemäß Art. 12. MAR, 1ª edição, Berlin, Duncker & Hublot, 2020, p. 60.

256 ESMA, ESMA's technical advice on possible delegated acts concerning the Market Abuse Regulation, ESMA/2015/224, 3 de fevereiro de 2015, p. 78. Disponível em: https://www.esma.europa.eu/document/esma%E2%80%99s-technical-advice-possible-delegated-acts-concerning-market-abuse-regulation (consultado em 05/05/2022).

gociação expressiva para fins de expressão política, social, ou estética[257]. Os negociadores expressivos sabem que o movimento do preço das ações que geram não reflete os fundamentos das ações, e que podem incorrer em perdas quando a correção dos preços ocorrer[258]. No entanto, consideram que os seus atos expressivos valem o risco de quaisquer perdas associadas[259].

Há outros problemas, tais como distinguir, dentro de uma estratégia, quem negoceia com intenção de manipular o preço com vista à obtenção de lucro e quem o faz sem intenção de obter lucro. Dentro de uma estratégia de NCIRRS podem também haver vários motivos, sendo claro que o objetivo será único: influenciar os preços de certo instrumento financeiro.

e) A execução coletiva por parte dos investidores de retalho

No entanto, é problemático que o comportamento individual de cada investidor de retalho não tenha por si só a aptidão para enviar uma indicação enganadora ou para causar um nível artificial de preços[260]. Ou seja, a manipulação de mercado apenas se pode verificar se todos os participantes da NCIRRS efetivarem a negociação de acordo com a estratégia, uma vez que a negociação individual de cada investidor de retalho não tem aptidão para a manipulação de mercado. Apenas considerando o conjunto das transações desses investidores é que as transações podem, no mínimo de forma provável, dar indicações enganosas, ou produzir preços anormais ou artificiais.

A estratégia de colocação de ordens em sentido comum (incluindo a negociação de instrumentos financeiros diferentes, mas cujos preços estão interligados, como ações e contratos de opções, tal como no caso GME) pelos diversos investidores de retalho é uma condição fundamental para o alcançar do objetivo da NCIRRS. Por sua vez, o alcançar do objetivo da negociação coordenada implica a produção de efeitos que, atendendo ao grau de sucesso da mesma e do número de investidores envolvidos, podem variar entre a produção de uma indicação enganosa ou de produção de preços que se desviam do preço que seria formado pela livre interação entre procura e oferta.

No que diz respeito ao requisito de conexão entre os investidores de retalho, seguimos a posição de Alexander Sajnovits, segundo a qual, de acordo com a lógica sistemática da lei aplicável, os requisitos de aptidão do conluio do art. 12.º nº1 alínea a) do MAR não devem ser mais baixos do que os estabelecidos

---

257 John Anderson, Jeremy Kidd e George Mocsary, "Social Media, Securities Markets, and the Phenomenon of Expressive Trading", 25 Lewis & Clark L. Rev. 1223, 2022, p. 11, disponível em: https://ssrn.com/abstract=3834801,

258 John Anderson, Jeremy Kidd e George Mocsary, "Social Media, Securities Markets, and the Phenomenon of Expressive Trading", 25 Lewis & Clark L. Rev. 1223, 2022, p. 12, disponível em: https://ssrn.com/abstract=3834801, .

259 Ibid.

260 Rüdiger Veil e Lena Templer, "GameStop, Reddit und die Hedgefonds - Betrachtungen aus der Perspektive des europäischen Kapitalmarktrechts", *ZIP*, 2021, p. 986.

no art. 12.º n.º 2 alínea a) do mesmo regulamento.[261] Como tal remetemos para a análise deste requisito realizada no ponto 2.2 do presente capítulo.

Até aqui, vimos que efetiva negociação dos investidores de retalho de acordo com a estratégia coletiva pode preencher quase todos os requisitos do art. 12.º nº1 a) i) e ii) do MAR, tendo concluído, através da consideração dos factos dos casos GME e das "ações *meme*", que a efetiva negociação coletiva pode (i) emitir indicações falsas ou enganosas a um investidor razoável na medida em que um investidor razoável toma em consideração as indicações dos efeitos provocados pela negociação coordenada como emitindo novas informações que, na realidade, não existem e não correspondem à verdade; e (ii) influenciar os preços, contribuindo para que estes atinjam níveis anormais ou artificiais, na medida em que se afastam dos seus valores fundamentais e dos normais mecanismos de formação de preço. Como tal sobra apenas o difícil requisito da conexão, uma vez que a negociação de cada investidor de retalho participante individualmente não tem aptidão para, pelo menos de forma provável, influenciar os preços.

5.2. ART. 12.º N.º 2 ALÍNEA A) DO MAR

Cabe agora a análise da aplicação da alínea a) do n.º 2 do art. 12.º do MAR, que, tal como previamente referido, em caso de verificação dos requisitos elencados dificilmente pode ser excluída. Na referida alínea é estabelecida a classificação do chamado *abusive squeeze*[262] como prática manipuladora de mercado onde, de forma concertada, uma pessoa ou pessoas asseguram uma posição dominante sobre um instrumento financeiro. O *abusive squeeze* consiste em tirar vantagem da influência significante sobre a procura, ou a oferta, de instrumentos financeiros para distorcer os preços[263].

Por outro lado, um *abusive squeeze* no sentido da referida alínea pode também violar a proibição de abuso de posição dominante do Direito da Concorrência, estabelecida no art. 102º do Tratado de Funcionamento da União Europeia (doravante TFUE), uma vez que sejam impostas condições de transação não equitativas ou se fixem preços de compra ou venda[264].

---

261 Alexander Sajnovits, "GameStop im Lichte der MAR – Meme-Trading, soziale Medien und Handelsbeschränkungen durch Broker", *Zeitschrift für Unternehmens- und Gesellschaftsrecht*, vol. 50, n.º 5, 2021, p. 822 (pp. 804–845).

262 O *abusive squeeze* é também estabelecido na alínea b) do parágrafo 2 da Secção I do Anexo II do Regulamento Delegado 2016/522 como indicador para o art. 12.º n.º 1 alínea a) do MAR por via do indicador A alínea a) do anexo I do Regulamento (UE) n.º 596/2014.

263 Lars Teigelack, "Market Manipulation" *in* Rüdiger Veil, *European Capital Markets Law*, 2ª edição, Oxford, Hart Publishing, 2017, p. 237.

264 Art. 102º do TFUE: «É incompatível com o mercado interno e proibido, na medida em que tal seja suscetível de afetar o comércio entre os Estados-Membros, o facto de uma ou mais empresas explorarem de forma abusiva uma posição dominante no mercado interno ou numa parte substancial deste. Estas práticas abusivas podem, nomeadamente, consistir em: a) Impor, de forma direta ou indireta, preços de compra ou de venda ou outras

Assim, são as normas concorrenciais e dos mercados financeiros aplicáveis paralelamente[265].

Visto que no caso GME se verificou o *short squeeze* de fundos de investimento de alto retorno[266] é adequada a ponderação da aplicação desta alínea. Sublinha-se que os apertos abusivos levam ao aperto do mercado, reduzindo assim a liquidez e aumentando os custos de transação implícitos de todos os participantes no mercado[267]. Isto reduz a eficiência dos preços e torna o mercado mais volátil[268], contribuindo para diminuir a confiança dos investidores no mercado. Relembra-se que tendo acontecido no caso GME, pode ser um episódio possível no âmbito da NCIRRS.

Nos termos do art. 12.º n.º 2 alínea a) do MAR, são consideradas como manipulação de mercado atividades realizadas com o fim de assegurar uma posição dominante no que respeita à oferta ou procura de um instrumento financeiro por uma ou várias pessoas agindo de forma concertada e se tiverem como consequência real, ou provável, a fixação direta ou indireta do preço de compra ou venda ou de outras condições de negociação não equitativas[269].

a) A posição dominante

O legislador europeu estabeleceu no artigo em questão o requisito de obtenção de uma posição dominante sobre a oferta ou procura de um instrumento financeiro, sem, no entanto, especificar quando se verifica tal obtenção de uma posição dominante.

Para uma determinação mais detalhada da existência de uma posição dominante, no que diz respeito à delimitação do mercado e ao grau de domínio, a opinião predominante é a favor de que sejam seguidos os critérios desenvolvidos nas normas do Direito da Concorrência[270].

condições de transação não equitativas; b) Limitar a produção, a distribuição ou o desenvolvimento técnico em prejuízo dos consumidores; c) Aplicar, relativamente a parceiros comerciais, condições desiguais no caso de prestações equivalentes colocando-os, por esse facto, em desvantagem na concorrência; d) Subordinar a celebração de contratos à aceitação, por parte dos outros contraentes, de prestações suplementares que, pela sua natureza ou de acordo com os usos comerciais, não têm ligação com o objeto desses contratos.»

265 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 591.

266 Ver *supra*, Capítulo I 1.

267 Larry Harris, *Trading & Exchanges*, 1ª edição, Oxford, Oxford University Press, 2002, p. 256

268 Franklin Allen, Lubomir Litov e Jianping Mei, "Large Investors, Price Manipulation, and Limits to Arbitrage: An Anatomy of Market Corners", *Review of Finance*, Vol. 10, n.º 4, 2006, p. 678 (pp. 645-693).

269 Artigo 12.º n.º 2 alínea a) do Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

270 Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005, p. 168.

É de sublinhar, porém, que a casuística do Direito da Concorrência não pode ser diretamente adotada devido aos diferentes objetivos de proteção que prossegue quando comparada com as especificidades dos mercados financeiros[271].

Contudo, a utilização de componentes do Direito da Concorrência representa ganhos, pelo menos, no que diz respeito à delimitação de mercado e ao grau de controlo[272]. Estes são úteis em substância para efeitos da proibição de manipulação do mercado pois a possibilidade de existência de uma posição dominante e, portanto, também de uma posição potencialmente influenciadora dos preços em relação a um objeto de referência, depende de condições prévias muito semelhantes tanto nos diferentes mercados de produtos como nos mercados financeiros[273].

Para a determinação da posição dominante de acordo com o estabelecido à luz do Direito da Concorrência deve ser definido o mercado relevante[274]. Assim, o mercado relevante é definido de acordo com três parâmetros: o produto em questão, a dimensão geográfica e a dimensão temporal[275]. Para tal é necessário, no quadro da substituibilidade do produto, questionar quais os produtos que, do lado da procura, são substituíveis[276].

No caso GME, os detentores de posições curtas em ações da GME não tinham possibilidade de comprar instrumentos financeiros de outras empresas para fechar a sua posição. O mercado relevante irá, então, para o respetivo período temporal ser o mercado para a compra do concreto instrumento financeiro. Portanto, neste caso, o mercado relevante será o mercado de ações da GME. Aqui deve relevar-se a ligação dos contratos de opções sobre as ações com o mercado das respetivas ações uma vez que estes estão interligados, produzindo as variações num deles efeitos também no restante. Isto significa que os investidores podem indiretamente exercer uma influência no mercado dos respetivos valores mobiliários sem deterem os valores mobiliários, tal como se verifica no caso GME[277]. Neste caso, a nosso ver, deve-se, como tal, ter em consideração as posições nos instrumentos financeiros derivados com ligação ao instrumento financeiro principal em análise para a determinação da quota de mercado, para efeitos de avaliação

---

271 Alexander Sajnovits, "GameStop im Lichte der MAR – Meme-Trading, soziale Medien und Handelsbeschränkungen durch Broker", *Zeitschrift für Unternehmens- und Gesellschaftsrecht*, vol. 50, n.º 5, 2021, p. 813 (pp. 804–845).

272 Ibid.

273 Alexander Sajnovits, "GameStop im Lichte der MAR – Meme-Trading, soziale Medien und Handelsbeschränkungen durch Broker", *Zeitschrift für Unternehmens- und Gesellschaftsrecht*, vol. 50, n.º 5, 2021, p. 813 (pp. 804–845).

274 Miguel Moura e Silva, *Direito da Concorrência*, 2ª edição, Lisboa, AAFDL Editora, 2018, pp. 883 e ss.

275 Ibid.

276 Ibid.

277 Ver *supra*, Capítulo I.

da produção de efeitos passíveis de subsunção à alínea a) do n.º 2 do art. 12.º do MAR.

Para determinar se no mercado relevante em causa se verifica uma posição dominante será necessário olhar à quota de mercado, a qual, se especialmente alta, indiciará uma posição dominante no respetivo mercado[278]. No entanto, uma quota de mercado mais baixa poderá chegar se do lado da procura não são encontradas alternativas na quantidade necessária de modo que os preços são controlados por quem detém a posição dominante no mercado[279]. No caso GME, como referido, dificilmente os investidores de retalho conseguiram uma posição dominante sob uma perspetiva da quota maioritária de mercado. Porém, a quota mais baixa que os mesmos obtiveram terá sido suficiente para influenciar consideravelmente os preços e provocar o *short squeeze* dos grandes fundos de investimento de alto retorno[280]. Para tal devemos, como referido, considerar as posições dos contratos de opções e outros instrumentos derivados que às ações estejam ligadas.

Por conseguinte, como demonstra o caso GME, tomando em consideração o grande poder de oferta e procura que os investidores de retalho podem obter, pelo menos de forma concertada, através da compra e venda de ações e de contratos derivados, como contratos de opções, é certamente possível que um grau de domínio suficiente para uma posição dominante num mercado relevante (instrumento subjacente) seja atingido[281].

Uma posição cética a este respeito, apresentam Maximilian Merwald e Pirmin Schauer. Estes defendem que devido à natureza *antitrust* da norma, faz sentido analisar através dos instrumentos de medida do poder de mercado estabelecidos no Direito da Concorrência Europeu, tal como a quota de mercado[282]. Assim, no caso de empresas de capitalização elevada dificilmente investidores de retalho em concertação conseguirão obter uma quota de mercado suficientemente elevada para controlar toda a procura[283]. Ainda assim, os autores reconhecem que, no caso GME, os investidores de retalho através da sua negociação coordenada influenciaram os preços das ações da GME.

---

278 Parágrafo 13 e ss. da Comunicação da Comissão, Orientação sobre as prioridades da Comissão na aplicação do artigo 82.º do Tratado CE a comportamentos de exclusão abusivos por parte de empresas em posição dominante. Ver Miguel Moura e Silva, *Direito da Concorrência*, 2ª edição, Lisboa, AAFDL Editora, 2018.

279 Ibid.

280 Ver *supra*, Capítulo I.

281 Rüdiger Veil e Lena Templer, "GameStop, Reddit und die Hedgefonds - Betrachtungen aus der Perspektive des europäischen Kapitalmarktrechts", *ZIP*, 2021, p. 986.

282 Maximilian Merwald e Pirmin Schauer, "Marktmanipulation, Social Media und Noise Trader im Fall GameStop", *BKR*, 2021, p.287 (p.280-292).

283 Christian Schröder, *Handbuch Kapitalmarktstrafrecht*, 3ª edição, Heymanns Verlag GmbH, 2015, § 20 a WpHG parágrafo 504.

No entanto, consideram-na uma influência que não resulta de um poder de mercado no sentido de uma posição dominante capaz de ditar os preços[284].

No entanto, a nosso ver, é de sublinhar que o alcance das redes sociais é ainda imprevisível e que, como recentes estudos do caso GME demonstram, estes números podem ter impactos bastante significativos[285]. Além disso, um controlo de toda a procura e oferta por investidores de retalho, tal como Maximilian Merwald e Pirmin Schauer afirmam, é altamente improvável, mas não exclui a obtenção de uma quota que permita um grau de domínio suficiente para exercer influência na formação dos preços nos mercados financeiros, pois, tal como referido, o alcance das redes sociais é difícil de prever e o caso GME demonstra já o exercício de uma significativa influência nos preços através da NCIRRS. Por outro lado, será importante perceber qual o requisito mínimo para a obtenção de uma posição dominante, sendo que se for a capacidade de ditar unilateralmente preços, então os investidores de retalho em negociação coordenada através das redes sociais provavelmente não conseguirão obter uma quota de mercado que tal capacidade atribua. Para ilustrar esta ideia, tenha-se em consideração que nos mercados de capitais dos Estados Unidos da América, cerca de 80% do capital pertence a investidores institucionais[286].

Klaus Schmolke afirma que decisiva para o estabelecimento do poder de mercado será a verificação da possibilidade da parte do manipulador de fixar os preços de forma unilateral[287]. Seguindo esta perspetiva, a nosso ver os investidores de retalho em coordenação através das redes sociais não obtiveram uma posição dominante visto que não tiveram a possibilidade de unilateralmente fixar preços. Aplicando à negociação coordenada de investidores de retalho através das redes sociais, muito dificilmente conseguirão estes obter os números e capital suficiente para obter uma posição de tal forma dominante que lhes permita ditar unilateralmente os preços.

No entanto, nós defendemos uma interpretação mais extensa da norma no sentido da consideração de uma quota de mercado capaz de produzir efeitos consideráveis no preço como compatível com a letra da norma, preenchendo o requisito da posição dominante. Mesmo não detendo uma posição dominante no sentido de uma capacidade de ditar unilateralmente

---

284 Maximilian Merwald e Pirmin Schauer, "Marktmanipulation, Social Media und Noise Trader im Fall GameStop", *BKR*, 2021, p.287 (p.280-292).

285 Ver Joshua Mitts *et al*., "A Report by the Ad Hoc Academic Committee on Equity and Options Market Structure Conditions in Early 2021", 2022, disponível em: https://ssrn.com/abstract=4030179. Franklin Allen *et al*., "Squeezing Shorts Through Social Media Platforms", *Swiss Finance Institute Paper n.º 21-31*, 2021, disponível em: https://ssrn.com/abstract=3823151, Ver também *supra*, Capítulo I.

286 Pensions & Investments. Disponível em:https://www.pionline.com/article/20170425/INTERACTIVE/170429926/80-of-equity-market-cap-held-by-institutions (consultado em 29 de abril de 2022).

287 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 590.

preços, no caso GME observou-se uma quota de detenção de ações da GME e instrumentos derivados cujo valor base são as ações da GME que permitiu exercer influência nos preços com o objetivo de distorcer os preços e criar condições de negociação não equitativas para as partes com posições de venda a descoberto.

Quanto à duração da posição dominante, o legislador contenta-se com a obtenção desta, mesmo que apenas temporariamente, podendo tal posição ser obtida através de uma única pessoa ou de várias pessoas em conluio (a chamada *posição dominante coletiva*, prevista no art. 102º do TFUE)[288]. Sublinha-se que o legislador se basta com a obtenção de tal posição, pelo que não é necessária qualquer utilização da posição dominante ou uma intervenção intencional sobre o preço[289].

A obtenção de uma posição dominante capaz de influenciar o preço deve ser previsível para a parte que a obtém, uma vez que também a livre interação das forças de procura e oferta pode conduzir a um aperto de mercado, sendo assim possível distinguir um aperto natural de um *abusive squeeze*[290]. Apesar do critério da previsibilidade, visto que o legislador não acrescentou um requisito subjetivo, não é de considerar que seja necessária intenção de obtenção de posição dominante.

No caso GME, visto que os investidores de retalho coordenaram e aplicaram uma estratégia conjunta com vista a influenciar os preços, a obtenção de uma posição dominante é, para estes, no mínimo, previsível. O mesmo é aplicável à NCIRRS em geral.

b) Ação de forma concertada

O legislador europeu refere expressamente «pessoas agindo de forma concertada». No entanto, ainda não foi clarificada a forma como deve ser definida com mais pormenor essa atuação concertada, na aceção do artigo 12.º n.º 2 alínea a) do MAR[291].

Da NCIRRS e dos factos do caso GME e das "ações *meme*", retira-se que os investidores de retalho discutem inicialmente nas redes sociais sobre instrumentos financeiros, avançando posteriormente para uma estratégia de negociação coordenada na crença de, em conjunto, conseguirem produzir alterações nos preços, e conquistando posteriormente novos investidores de retalho que vão aderindo à estratégia à medida que esta se desenrola.

Portanto, muitos investidores de retalho discutem através das publicações e mensagens nas redes sociais, às quais se seguem publicações com

288 Ibid.

289 Ibid.

290 Milan Bayram, Manipulative Handelspraktiken gemäß Art. 12. MAR, Berlin, 1ª edição, Berlin, Duncker & Hublot, 2020, p. 150.

291 Rüdiger Veil e Lena Templer, *GameStop, Reddit und die Hedgefonds - Betrachtungen aus der Perspektive des europäischen Kapitalmarktrechts*, ZIP 2021, p. 986.

o intuito de coordenar a negociação no sentido de um objetivo comum. No entanto, provavelmente, a grande maioria dos investidores envolvidos não pronunciarão a sua aceitação através de uma publicação, mensagem ou partilha, comportando-se antes passivamente. Acrescenta-se que as identidades dos investidores nas redes sociais são em regra desconhecidas. Mesmo emitindo os utilizadores declarações expressas de aceitação e adesão à negociação coordenada, numa rede social com milhões de utilizadores, em regra, anónimos, tal dificilmente provocaria obrigações mútuas *de facto* de concretizar determinada negociação[292].

A este propósito, a falta de uma obrigação *de facto* mútua de concretização das transações da parte dos investidores de retalho envolvidos é um problema, pois, tal como apontam Maximilian Merwald e Pirmin Schauer, dentro do coletivo de investidores de retalho organizados através das redes sociais, para cada investidor individual será imprevisível se e quando os restantes poderão abandonar a estratégia[293]. Como tal, devem os investidores envolvidos temer o oportunismo dos restantes, uma vez que a estratégia de negociação coordenada pode falhar caso alguns investidores efetuem transações em sentido contrário do acordado[294].

Tomemos como exemplo um caso como o da GME, em que os investidores de retalho em negociação coordenada pretendam influenciar os preços de modo a expressar revolta e prejudicar um fundo de investimento de alto retorno. Na fase em que o curso das ações da empresa se encontrava num dos pontos mais elevados, bastaria que um número considerável (mas que não necessita de ser maioritário) dos investidores de retalho envolvidos na estratégia de negociação coordenada optassem por vender, de modo a obterem lucro, para que a estratégia perdesse efeito, pois as vendas iriam voltar a pressionar os preços num sentido descendente[295].

Neste sentido, Maximilian Merwald e Pirmin Schauer chamam a atenção que para o poder de fixação de preços é necessária uma coesão interna mais forte, que, em caso de dúvida, supera também o eventual oportunismo pessoal que pode surgir entre os investidores de uma negociação coordenada[296]. A nosso ver, convém diferenciar entre coesão necessária para a

---

[292] Alexander Sajnovits, "GameStop im Lichte der MAR – Meme-Trading, soziale Medien und Handelsbeschränkungen durch Broker", *Zeitschrift für Unternehmens- und Gesellschaftsrecht*, vol. 50, n.º 5, 2021, p. 814 (p. 804–845).

[293] Maximilian Merwald e Pirmin Schauer, "Marktmanipulation, Social Media und Noise Trader im Fall GameStop", *BKR*, 2021, p. 287 (pp. 280-292).

[294] Ibid.

[295] Neste exemplo, à semelhança do caso GME e das "ações *meme*", a negociação coordenada pressiona os preços a subir. No entanto, podem também, por exemplo, surgir estratégias no sentido de uma influência dos preços em sentido descendente, onde os meios dos investidores de retalho sejam vendas curtas e derivados de opções. Os objetivos podem também ser diferentes.

[296] Maximilian Merwald e Pirmin Schauer, "Marktmanipulation, Social Media und Noise Trader im Fall GameStop", *BKR*, 2021, p. 287 (pp. 280-292).

fixação de preços e coesão necessária para a influência de preços. Embora reconhecendo que para a fixação de preços será necessária uma coesão interna mais forte, para a qual não deverão chegar meras declarações de apoio, sob diversas formas, da parte dos investidores de retalho nas redes sociais, o caso GME demonstra que não é necessária uma coesão interna mais forte para exercer uma influência considerável sobre os preços com efeitos contrários aos objetivos defendidos pelas normas europeias dos mercados financeiros. Neste sentido, não consideramos ser necessária uma tal coesão interna com imposição de obrigações mútuas entre os investidores de retalho para que estes consigam influenciar os preços.

Poderia ser útil a consideração de uma declaração tácita de aceitação para a participação na negociação coordenada através das redes sociais, declaração essa cuja aceitação pelos investidores seria expressa através da realização das efetivas transações de acordo com a estratégia definida na rede social. Assim, deduzir-se-ia que o facto da concretização da negociação de acordo com a estratégia propagada na rede social revela com grande probabilidade aquela declaração.

Esta solução não está, porém, livre de grandes problemas. O maior problema prende-se com a investigação desta adesão tácita à negociação coordenada, uma vez que é questionável se a negociação no sentido da estratégia bastará para uma inclusão automática na mesma. Um investidor sem ligação à estratégia pode também decidir negociar de forma idêntica sem a partilha do mesmo objetivo. Já numa NCIRRS com diversas instruções e fases de negociação coordenada, confirmando-se que um investidor negoceia de acordo com todas estas fases, a probabilidade de esse investidor ser participante seria bastante elevada. Acresce que os custos de implementação de tal investigação seriam também bastante avultados.

Por outro lado, a investigação é muito difícil atendendo ao número de participantes numa negociação coordenada através das redes sociais, que pode atingir números nas ordens de centenas de milhares ou milhões de pessoas espalhadas por todo o globo, sujeitas a diferentes ordenamentos jurídicos.

A ausência de uma ligação vinculativa entre os participantes não exclui a possibilidade do exercício de influência significativa no preço através da negociação coordenada de grandes números de investidores de retalho. Além disso, redes sociais como o fórum WSB da rede *Reddit*, permitem que estes investidores atinjam, como referido, um grande número, tendo em conjunto efeitos comparáveis aos de um grande investidor institucional em termos de impacto da sua negociação. Estudos de reputadas instituições e académicos apontam no referido sentido[297].

[297] Ver Joshua Mitts *et al*., "A Report by the Ad Hoc Academic Committee on Equity and Options Market Structure Conditions in Early 2021", 2022, disponível em: https://ssrn.com/abstract=4030179. Franklin Allen *et al*., "Squeezing Shorts Through Social Media Platforms", *Swiss Finance Institute Paper n.º 21-31*, 2021, disponível em: https://ssrn.com/abstract=3823151, Ver também *supra*, Capítulo I.

Mesmo tendo em conta o *telos* das normas dos mercados financeiros, e que a NCIRRS pode ter, tal como demonstrado no caso GME, consequências que prejudicam o bom funcionamento dos mercados financeiros e que ferem os objetivos defendidos pelo Direito dos Valores Mobiliários Europeu[298], o número de investidores de retalho que participam na NCIRRS pode, devido às razões referidas *supra*, constituir um obstáculo muito difícil de superar. Deste modo, a nosso ver, tanto a aplicação da alínea a) do número 1 do artigo 12.º como a alínea a) do número 2 do mesmo artigo caem devido à falha do requisito em questão.

c) Fixação de preços ou de condições de negociação não equitativas

Por último, o assegurar da posição dominante deve, pelo menos provavelmente, direta ou indiretamente fixar preços de instrumentos financeiros ou criar outras condições de negociação não equitativas. Relativamente à fixação de preços deve ser sublinhado que tal exige um grande poder de mercado que, regra geral, estará apenas ao alcance de grandes empresas[299].

No entanto, e em alternativa, é suficiente que através do assegurar da posição dominante se produzam, ou se possam provavelmente produzir, outras condições de negociação não equitativas. Tal abrange, em última análise, todas as deficiências das condições de mercado relacionadas com o poder de mercado para além do controlo dos preços[300].

No caso GME, a NCIRRS com ações e instrumentos financeiros derivados influenciou os preços de modo considerável, desviando-os dos valores fundamentais e conduzindo ao *short squeeze* de fundos de investimento de alto retorno que detinham posições curtas, causando elevada volatilidade e prejudicando a liquidez e a confiança nos mercados.

Os investidores de retalho "apostaram" na GME através da aquisição de ações e de contratos de opções. Estas causaram, como explicado *supra*[301], *short squeeze* e *gamma squeeze*. À medida que, em consequência destes, o preço das ações da GME subiu, os detentores de posições a descoberto foram obrigados a fechar as suas posições a fim de reduzirem os seus prejuízos. No entanto, não só os grandes fundos de capitais sofreram grandes perdas, resultando a elevada volatilidade[302] também em relatos de avultados prejuízos do lado dos pequenos investidores de retalho.[303]

---

298 Ver *supra*, Capítulo II 2.

299 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 591.

300 Ibid.

301 Ver *supra*, Capítulo I 1.

302 Entre janeiro e fevereiro deu-se uma acentuada queda dos preços - a *GameStop* apresentava um curso de 40 dólares americanos em meados de fevereiro de 2021.

303 Rachel Ensign, "GameStop Investors Who Bet Big—and Lost Big", Wall Street Journal, disponível em: https://www.wsj.com/articles/gamestop-investors-who-bet-bigand-lost-big-11613385002 (consultado em 21 de junho de 2021).

Como tal, a criação de condições de negociação no mínimo não equitativas foi atingida, pelo que este requisito se verifica. Aplicando à NCIRRS, para a verificação deste requisito terão de produzir-se condições não equitativas ou fixar-se os preços de instrumentos financeiros. Deve também relevar-se que uma verificação da probabilidade antes da produção de quaisquer efeitos é bastante difícil, tendo em conta a imprevisibilidade dos números e correspondentes consequências de uma NCIRRS.

Assim, concluímos que a NCIRRS preenche todos os requisitos de aplicação do art. 12.º n.º 2 alínea a) do MAR, com exceção do requisito da conexão das pessoas envolvidas. A NCIRRS do caso GME obteve, a nosso ver, uma posição dominante, uma vez que através da negociação de ações da GME e de instrumentos derivados, cujo ativo base são as ações da GME, influenciou, intencionalmente, significativamente os preços, distorcendo-os (afastando-os dos seus valores fundamentais) e, gerando, deste modo, condições não equitativas que levaram ao *short squeeze* de partes com posições de venda a descoberto.

Por outro lado, a aplicação da alínea d) do n.º 2 esbarra, à semelhança da alínea a) do n.º 1 do mesmo artigo, nas dificuldades de aplicação do requisito da ação concertada, atendendo ao número de participantes envolvidos que podem estar espalhados por diferentes países e diferentes ordenamentos jurídicos, comportando a investigação da participação custos enormíssimos e não sendo clara a existência de um método eficaz a utilizar para determinar quais os investidores de retalho participantes.

6. AS PUBLICAÇÕES DA NEGOCIAÇÃO COORDENADA NAS REDES SOCIAIS

Neste capítulo, a nossa análise foca-se no possível enquadramento das publicações nas redes sociais que possibilitam e estimulam a negociação coordenada nas redes sociais nas normas de manipulação de mercado do artigo 12.º do MAR.

Como referido no Capítulo I, os investidores começam por discutir nas redes sociais, seguindo-se uma fase de coordenação estratégica para negociação de instrumentos financeiros, nos quais os intervenientes acreditam poder influenciar o preço, seguindo-se que à medida que, em resultado da negociação coordenada, os volumes dos instrumentos financeiros começam a aumentar, mais investidores começam a reparar nas indicações nas redes sociais, juntando-se à estratégia. Daqui retiramos dois tipos de publicações capazes de desencadear e coordenar a negociação coordenada nas redes sociais: as publicações no âmbito da discussão, e as publicações que coordenam a estratégia de negociação. Estas serão analisadas no âmbito da manipulação de mercado através da informação do art. 12.º n.º 1 alínea

c) do MAR e da manipulação de mercado através da informação e negociação da alínea b) do mesmo n.º 1 do mesmo artigo.

6.1. ART. 12.º N.º 1 ALÍNEA C) DO MAR

A manipulação de mercado do art. 12.º n.º 1 alínea c) do MAR[304] pode ser aplicável se, com publicações nas redes sociais, for divulgada informação que dê indicações falsas ou enganosas relativamente à oferta ou ao preço de instrumentos financeiros ou que fixe os preços a níveis artificiais, acrescentando-se o requisito subjetivo de a pessoa que procedeu à divulgação ter sabido, ou dever ter sabido, que as informações eram falsas ou enganosas. Como já referido, a informação é um dos mais importantes motivos de negociação dos participantes nos mercados financeiros e uma das razões pelas quais a eficiência de mercado é tao importante[305]. Nesse sentido, o legislador procura evitar, através do art. 12.º n.º 1 alínea c) do MAR, que a divulgação de informações falsas ou enganosas influencie o preço dos instrumentos financeiros e prejudique a integridade do mercado.[306]

a) Divulgação de informações

O termo "informação" é geralmente entendido num sentido lato, e pode também incluir meros juízos de valor, previsões ou recomendações, abrangendo deste modo a transmissão de dados sob qualquer forma[307]. Tal abrangência permite também, a nosso ver, englobar as imagens *meme* como uma forma de informação no âmbito do art. 12.º n.º 1 alínea c) do MAR, visto que imagens deste tipo são aptas a transmitir dados.

As informações não têm necessariamente de conter factos, pelo que rumores, previsões e juízos de valor sem um núcleo factual são também suficientes para a abrangência do art. 12.º n.º 1 alínea c) do MAR[308].

---

304 Para uma análise da manipulação de mercado através da informação sob uma perspetiva de Direito Penal, ver Duarte Roseiro, "As sociedades de notação de risco e o crime de manipulação do mercado", 2017, disponível em: https://run.unl.pt/handle/10362/20346

305 Ver *supra*, Capítulo II. O legislador reconhece também este "poder da informação como meio de atuação sobre o mercado", razão pela qual estabelece a manipulação através da informação. Alexandre Brandão da Veiga, *Crime de Manipulação, Defesa e Criação de Mercado*, 1ª edição, Coimbra, Almedina, 2001, p. 41. "A tutela da informação nos mercados de valores mobiliários é feita através de um completo regime sancionatório contraordenacional e, para as condutas dotadas de maior danosidade, é reservada a tutela penal." Duarte Roseiro, "As sociedades de notação de risco e o crime de manipulação do mercado", 2017, p. 32, disponível em: https://run.unl.pt/handle/10362/20346

306 Considerandos 4 e 47 frase 1 do Regulamento (UE) n.º. 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

307 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 570.

308 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 571.

A informação deve ainda ser disseminada, i. e., esta deve ser tornada publicamente acessível, (pelo menos de forma provável) de modo a que um grande número de pessoas dela possam tomar conhecimento[309]. Neste ponto, mostra-se o legislador europeu já consciente do potencial de disseminação da *Internet* e das redes sociais, sendo a disseminação por essas vias abrangida pela alínea c) e no considerando 48 do MAR[310].

No caso GME e das "ações *meme*", frequentemente, as publicações dos investidores de retalho nas redes sociais, em âmbito de discussão ou transmissão de indicações para uma coordenação, ocorreram sob diversas formas, entre as quais as de texto ou mensagem, vídeo ou imagem *meme*. Quanto às publicações sob a forma de texto, mensagem ou vídeo é mais fácil a análise de uma possível transmissão de informação aos investidores, visto que contêm normalmente um texto escrito ou narrado. Por outro lado, a imagem *meme* também transmite informação, apesar de tal não parecer tão óbvio visto que não há um conteúdo textual escrito (como nas publicações de texto ou mensagem) ou narrado (como nas publicações de vídeos). Nas imagens *meme* há, normalmente, apenas uma curta descrição ou título que conjugados com a imagem transmitem informação. Por exemplo, o *meme* "*Diamond Hands*"[311] transmitia a indicação no sentido da manutenção de uma posição longa no instrumento financeiro, mesmo em períodos de elevada volatilidade.

Tomando em consideração a simplicidade da combinação de imagens e curtas descrições ou títulos utilizados nas imagens *meme*, num contexto de discussão ou fórum destinado à discussão de investimento, é razoável assumir que um investidor compreenderá a indicação que este tipo de imagem contém, podendo assim estas também ser aptas a transmitir informação. Tal está sujeito à verificação do contexto de inserção num local de discussão sobre investimento ou relacionado. Sendo as publicações dos investidores de retalho partilhadas em sítios das redes sociais, estas serão disseminadas e tornadas publicamente acessíveis, delas tomando conhecimento qualquer pessoa que aceda à respetiva rede social ou sítio de *Internet* onde a publicação se verifique. Nas redes sociais e Internet um utilizador facil-

309 ESMA, Final Report, Draft Technical standards on the Market Abuse Regulation, 28 de setembro de 2015, ESMA/2015/1455, p. 72. Disponível em: https://www.esma.europa.eu/sites/default/files/library/2015/11/2015-esma-1455_-_final_report_mar_ts.pdf (consultado em 10/05/2022).

310 Considerando 47 do Regulamento (UE) n.º. 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014: «Devido à utilização redobrada de sítios web, blogues e redes sociais, é importante esclarecer que a difusão de informações falsas ou enganosas através da Internet, nomeadamente em sítios de redes sociais ou blogues não atribuíveis, deverá ser considerada, para os fins do presente regulamento, equivalente a uma ação idêntica empreendida através de canais de comunicação mais tradicionais.».

311 Ver *supra*, Capítulo I 1.

mente perde o controlo dos destinatários da sua publicação, atingindo esta um número indeterminado e incontrolável de outros utilizadores.

É relevante, a este propósito, sublinhar que o número de pessoas a quem a informação chega influencia o seu potencial para influenciar o preço, sendo que para mercados de menor liquidez não é necessária a exigência de um número tão elevado de destinatários quanto o número de destinatários de uma informação no âmbito de um mercado de maior liquidez[312]. No caso da NCIRRS esta é uma questão relevante, pois não havendo um número de destinatários adequado a uma influência de preço no respetivo mercado, então não se verifica a componente da divulgação do requisito do conceito de informação. No caso GME não há dúvidas quanto a isto, visto que as informações chegaram a milhões de destinatários[313].

b) Indicações falsas ou enganosas quanto à procura ou preço de um instrumento financeiro

O legislador europeu impõe ainda que informações tenham como potencial efeito o de dar indicações falsas ou enganosas quanto à procura ou preço de um instrumento financeiro, ou fixar preços em níveis artificiais ou anormais.

A potencial indicação quanto ao preço de instrumentos financeiros e, indiretamente, acerca da sua procura e oferta verifica-se se um investidor razoável[314] provavelmente[315] tomaria em conta a informação para a sua decisão de investimento, visto que a informação, por sua vez, tem potencial para influenciar a procura e a oferta, ou o preço, de um certo instrumento financeiro[316].

A provável indicação dada pela referida informação deve ser falsa ou enganosa. Será falsa quando não corresponder à realidade do respetivo ins-

---

312 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 572.

313 O fórum WSB da rede *Reddit* conta com mais de doze milhões de utilizadores. https://www.reddit.com/r/wallstreetbets/

314 Como vimos, um investidor razoável é um investidor adequadamente informado, atento, com espírito crítico e familiarizado com as dinâmicas e acontecimentos dos mercados financeiros.

315 Quanto à questão das diferentes expressões utilizadas na versão de cada Estado-Membro da União Europeia, ver *supra* nota de rodapé 200. Para Duarte Roseiro "o que se exige é que em virtude de uma distorção da realidade provocada pelo ato de comunicação haja uma aptidão de alteração do comportamento dos seus destinatários em virtude dessa informação", acrescentando que a artificialidade se revela "por comparação àquele que seria o comportamento em caso de divulgação de informação correta". Duarte Roseiro, "As sociedades de notação de risco e o crime de manipulação do mercado", 2017, p. 43, disponível em: https://run.unl.pt/handle/10362/20346

316 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 575.

trumento financeiro. Será enganosa se é adequada para criar uma conceção errada da realidade a um investidor razoável[317].

É importante destacar ainda que indicações enganosas podem não apenas ser informações falsas, mas também informações de conteúdo correto que, devido à sua incompletude ou à forma imprecisa como são disponibilizadas dão origem a equívocos[318]. Tal justifica-se, uma vez que a incompletude ou imprecisão apresentam potencial para ocultar detalhes cujo conhecimento pode ser determinante para uma tomada de decisão por parte de um investidor[319].

No âmbito da NCIRRS, as publicações nas redes sociais que contenham informações sobre um determinado instrumento financeiro, ou a ele ligadas, poderiam, em termos do seu conteúdo, ser adequadas a dar indicações a um investidor razoável. Estas, de modo a se enquadrarem no âmbito de aplicação do art. 12.º n.º 1 alínea c) do MAR, deveriam ainda ser falsas ou enganosas. Portanto, para além de serem suscetíveis de serem tomadas em consideração por um investidor razoável para a sua tomada de decisão, as mesmas devem revelar factos, no mínimo, não verdadeiros sobre o instrumento financeiro em questão ou ter suscetibilidade de enganar um investidor razoável, através de factos falsos ou através da forma como é divulgada a respetiva informação.

No caso GME, foram várias as publicações nas redes sociais, nomeadamente no fórum WSB, com conteúdos não verdadeiros acerca da empresa GME, e que, como tal, seriam passíveis de serem tomadas em consideração pela generalidade dos investidores. Aqui, a questão principal a ser avaliada é se tais indicações, falsas ou enganosas, seriam tomadas em consideração por um investidor razoável. Tendo em conta, que as publicações são disseminadas em redes sociais, onde, na maior parte dos casos, os utilizadores não divulgam a sua identidade ou a mesma não é verificável, tal como se verifica com a maioria dos investidores de retalho nas redes sociais, nos casos GME e das "ações *meme*" não nos parece que um investidor razoável, familiarizado com os acontecimentos de mercado e com espírito crítico, tome em conta indicações, falsas ou enganosas, das publicações das redes sociais para a sua decisão de investimento. Não o fará, pois não tem meio de verificar a identidade do publicador ou de saber se este tem credibilidade

317 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 575. No mesmo sentido, para Frederico Costa Pinto, neste âmbito de informação falsa ou enganosa, inclui-se qualquer informação "sem uma correspondência exata com a realidade" ou que é apresentada "de uma forma que seja suscetível de induzir os destinatários em erro". Frederico Costa Pinto, *O Novo Regime dos Crimes e Contra-Ordenações no Código dos Valores Mobiliários,* 1ª edição, Coimbra, Almedina, 2000, p. 86. Ver também Alexandre Brandão da Veiga, *Crime de Manipulação, Defesa e Criação de Mercado*, 1ª edição, Coimbra, Almedina, 2001, pp. 42-47.

318 Ibid.

319 Ibid.

ou conhecimentos para publicar as informações em causa. Neste sentido aponta também Kilian Wegner, que vai um pouco mais longe ao referir que nem um investidor razoável (no sentido aqui presente) nem um investidor menos razoável, i. e., que negoceie com um certo grau de descuido[320], considerarão informações de fonte não fiável[321], não sendo em regra, deste modo, conduta manipulatória uma qualquer informação publicada sob pseudónimo num fórum de *Internet* ou rede social[322].

Kilian Wegner acrescenta, todavia, que, no caso de um utilizador ser reconhecido por um pseudónimo ou alcunha em determinado círculo, a probabilidade de aptidão de uma publicação aumenta[323]. Para tal, é necessário que a rede social onde o publicador é conhecido por esse pseudónimo ou alcunha esteja protegida por um sistema de segurança que não permita que a conta do referido publicador seja utilizada sem o seu conhecimento por outros utilizadores[324]. Um exemplo retirado do caso GME é o caso de Keith Gill[325], o utilizador que divulgou publicações nas quais realizou análises e avançou razões pelas quais acreditava no investimento nas ações da GME. A nosso ver, para um investidor razoável não chega que um utilizador conhecido divulgue e fundamente as suas crenças para que as suas indicações possam ser tomadas em consideração. Não nos parece que deixe de haver dúvidas relativamente à sua identidade, ou à fiabilidade dos seus conhecimentos. Como tal, um investidor razoável não tomaria em conta essas indicações para a sua tomada de decisão de investimento. O mesmo se aplica no caso de um utilizador conhecido pelo seu pseudónimo ou alcunha.

Por outro lado, temos ainda as publicações nas redes sociais que contenham instruções para a efetivação da NCIRRS. Neste caso, não nos parece que estas publicações deem indicações falsas ou enganosas, destinando-se a coordenar os participantes da NCIRRS. É o caso da publicação com a imagem *meme* de *Diamond Hands*[326], que instrui os investidores envolvidos a não venderem o instrumento financeiro apesar da elevada volatilidade do mercado. Já no caso da imagem *meme* de foguetão[327], esta é também uti-

---

320 Tipo de investidor que Kilian Wegner considera ser mais realista («noch ein „realistischer" (d. h. zu gewissem Grad auch zur Unvernunft neigender) Anleger (…)») Kilian Wegner, "Das „GameStop"-Phänomen nach deutschem Marktmissbrauchsrecht: Marktmanipulation oder legitimes Anlegerverhalten?", *BKR*, 2021, p. 183 (p. 181-188).

321 Kilian Wegner, "Das „GameStop"-Phänomen nach deutschem Marktmissbrauchsrecht: Marktmanipulation oder legitimes Anlegerverhalten?", *BKR*, 2021, p. 183 e 184 (p. 181-188).

322 Ibid.

323 Kilian Wegner, "Das „GameStop"-Phänomen nach deutschem Marktmissbrauchsrecht: Marktmanipulation oder legitimes Anlegerverhalten?", *BKR*, 2021, p. 184 (p. 181-188)

324 Ibid.

325 conhecido em algumas redes sociais como *@TheRoaringKitty.*

326 Ver *supra*, Capítulo I 1.2.

327 Ver *supra*, Capítulo I 1.2.

lizada no âmbito da NCIRRS para transmitir a informação de que irá ocorrer uma valorização no sentido de estimulação da efetivação da estratégia coordenada. Esta publicação poderia ser suscetível de transmitir a indicação de que um instrumento financeiro se está a valorizar. Nesse caso, se tal não correspondesse à verdade, a indicação seria falsa. Porém, como referido, um investidor razoável não tomará tal indicação em consideração.

c) Fixação de preços anormais ou artificiais

Em alternativa, o legislador europeu estabelece a possibilidade de verificação de uma manipulação de mercado através da informação, se esta, pelo menos de forma provável, pode fixar preços anormais ou artificiais.

Esta condição alternativa é relevante em relação à anterior se a informação não fornecer uma indicação falsa ou enganosa aos investidores, mas for, no entanto, apta, de forma provável, a fixar os preços a níveis artificias ou anormais. Pode ser o caso se uma publicação que dá instruções no âmbito de uma estratégia de negociação coordenada. No entanto, para tal exige-se a mesma probabilidade mínima que se exige na alínea a) do mesmo n.º 1 do art. 12.º do MAR[328].

Como visto no capítulo anterior, na análise do requisito da obtenção de preços artificiais ou anormais no âmbito do art. 12.º n.º 1 alínea a) do MAR, basta uma influência no preço de curto espaço temporal. Quanto ao conceito de preço artificial, este foi deixado em aberto pelo legislador europeu. A IOSCO avançou também com uma definição para a artificialidade dos preços, sendo esta «o desvio dos preços em relação às legítimas forças da oferta e da procura*».*[329] Esta, porém, deixa em aberto a questão acerca de quando um desvio do preço constituirá um legítimo comportamento de mercado, como parte da interação das forças de procura e oferta[330].

A nosso ver, olhando aos objetivos da regulação dos mercados financeiros, um preço artificial é aquele que se afasta do valor fundamental de um instrumento financeiro, o que tem graves implicações para a eficiência, liquidez e volatilidade e estabilidade dos mercados financeiros.

Vimos também que o método que, a nosso ver, mais vantagens apresenta na investigação dos preços é o método do estudo de casos, realizado por especialistas dos mercados financeiros, onde devem ser analisados os preços dos

---

328 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 576.

329 IOSCO, Investigating and Prosecuting Market Manipulation, maio de 2000, p. 13. «Price artificiality is the divergence of price from the legitimate forces of supply and demand. In order to establish price artificiality, it is therefore necessary to accumulate evidence that prices did not follow legitimate economic forces.». Disponível em: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD103.pdf

330 Daniel Fischel e David Ross, "Should Law Prohibit Manipulation?", Harvard Law Review, Vol.105, 1991, p.508 e 509.

respetivos instrumentos financeiros, bem como outros indicadores de grande relevo como a liquidez, a volatilidade ou os volumes de transação, e que no caso da NCIRRS deverão ser acompanhados da análise da atividade nas redes sociais relativamente a publicações nesse âmbito de práticas coordenadas.

De seguida, concluímos que, conforme demonstrado em diversos estudos[331], nos casos GME e das "ações *meme*" os preços resultantes da NCIRRS se afastaram consideravelmente dos valores fundamentais das respetivas ações, não resultando da normal interação entre as forças da procura e oferta, cumprindo-se, assim, o requisito da obtenção (no mínimo provável) de preços artificiais ou anormais.

Também as publicações nas redes socias que instruem a negociação coordenada (v.g. imagem *meme* de *Diamond Hands*), na medida que divulgam informações que levam à prossecução da negociação pelos investidores de retalho envolvidos na estratégia, podem produzir preços artificiais ou anormais. Tal justifica-se, pois, como analisado, a efetiva negociação levada a cabo pelos investidores de retalho cumpre o requisito da obtenção de preços anormais ou artificiais. Ora, sendo tal negociação resultante das publicações que as instruem, será lógico afirmar que as publicações no âmbito da NCIRRS cumprem o requisito da produção de preços artificiais ou anormais da alínea c) do número 1 do artigo 12.º do MAR. De mais difícil averiguação seria uma avaliação *ex ante* sobre a probabilidade de influência sobre os preços de modo a provocar uma distorção. O caso GME mostra que há uma probabilidade considerável para isso mediante a verificação de condições, tais como a participação de um número suficiente grande de investidores de retalho na estratégia.

d) Saber ou dever saber – o requisito subjetivo

O legislador europeu estabelece ainda um requisito subjetivo acerca do carácter da informação divulgada no art. 12.º n.º 1 c) do MAR, segundo o qual a pessoa que divulgou a informação sabia, ou devia saber, que a referida informação produz indicações falsas ou enganosas acerca do preço ou procura de um instrumento financeiro ou fixa o preço do mesmo em valores anormais ou artificiais. Do texto da norma («devia saber») retira-se que a negligência do publicador é suficiente para aplicação do art. 12.º n.º 1 alínea c) do MAR[332]. Tal analisa-se de forma objetiva, de acordo com o teste

---

331 Ver Franklin Allen *et al*., "Squeezing Shorts Through Social Media Platforms", *Swiss Finance Institute Paper n.º 21-31*, 2021, disponível em: https://ssrn.com/abstract=3823151, p. 35. Ver também *supra*, Capítulo I.

332 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, pp. 576 e 577. Para uma diferente interpretação, ver. Duarte Roseiro, "As sociedades de notação de risco e o crime de manipulação do mercado", 2017, pp. 44 e 45, disponível em: https://run.unl.pt/handle/10362/20346

da pessoa normal e racional: o que podia saber uma pessoa média normal e racional naquela situação concreta?[333]

No caso GME e das "ações *meme*", este requisito parece ser relativamente simples de aplicar. Visto que os investidores de retalho sabiam que com os diferentes tipos de publicações (discussão e instruções de negociação) emitiam indicações contrárias ao valor fundamental dos respetivos instrumentos financeiros, é possível concluir que estes sabiam, ou deviam saber, que com essas publicações poderiam ser produzidas indicações falsas ou enganosas ou com probabilidade de fixar o preço de um instrumento financeiro. Assim, nas publicações no âmbito da negociação coordenada através das redes sociais os publicadores devem, no mínimo, saber que estas podem ser aptas a produzir indicações falsas ou enganosas acerca da procura ou preço de instrumentos financeiros, ou a fixar preços em níveis anormais ou artificiais. Tal é mais evidente no caso das publicações que dão instruções para a negociação coordenada.

Encerramos esta secção concluindo que a primeira parte do art. 12.º n.º 1 alínea c) do MAR não é de aplicar às publicações nas redes sociais no âmbito da NCIRRS, visto que, apesar de estas poderem transmitir informação, as suas indicações falsas ou enganosas não serão tomadas em consideração por um investidor razoável. Isto porque este não tomaria em conta na sua decisão de investimento indicações provenientes de utilizadores de redes sociais, na sua maioria sem possibilidade de verificação da identidade e da fiabilidade dos seus conhecimentos.

Por outro lado, a segunda parte do art. 12.º n.º 1 alínea c) do MAR é a nosso ver aplicável, sendo as publicações no âmbito da NCIRRS, mediante a participação de um número suficientemente grande de investidores, aptas a transmitir, de forma provável, informação que levará os preços a atingirem níveis artificiais e anormais, desviando-os dos seus valores fundamentais e da normal interação entre as forças da procura e oferta. Em relação à efetiva negociação coordenada enquanto manipulação de mercado à luz do art. 12.º n.º 1 alínea a) do MAR, cuja aplicação poderá esbarrar na conexão entre os numerosos participantes da NCIRRS, a alínea c) tem a vantagem de a publicação ser realizada por apenas um participante (o participante que a publica), o que faz com que a aplicação desta não esbarre no problema da aplicação da alínea a) à efetiva prática de negociação coordenada devido ao número de participantes, nomeadamente no que toca à investigação e ao número de diferentes países e ordenamentos jurídicos que poderão estar envolvidos. Deste modo, as publicações que dão início e coordenam a NCIRRS podem ser consideradas como manipulação do mercado, violando a proibição da prática ou tentativa de manipulação de mercado do artigo 15.º do MAR.

---

333 Financial Conduct Autorithy, "MAR 1.8.5." *in FCA Handbook, 2016*, Disponível em: https://www.handbook.fca.org.uk/handbook/MAR/1/?view=chapter (consultado a 11/05/2022).

6.2. ART. 12.º N.º 1 ALÍNEA B) DO MAR

No artigo 12.º n.º 1 alínea b) do MAR, o legislador europeu define manipulação de mercado como qualquer "atividade ou conduta que afete, ou seja idónea para afetar, o preço de um ou mais instrumentos financeiros (…) recorrendo a procedimentos fictícios ou quaisquer outras formas de engano ou artifício"[334].

Esta variante da manipulação de mercado coloca particular ênfase no método de manipulação. O método da manipulação é aqui um comportamento que recorre a procedimentos fictícios ou quaisquer outras formas de engano ou artifício, as quais são, no mínimo, provavelmente adequadas a influenciar os preços dos instrumentos financeiros[335].

O Anexo I Secção B do MAR contém, por remissão do art. 12.º n.º 3, nas suas alíneas a) e b) duas concretizações de possíveis variantes de infração, com o objetivo de facilitar a interpretação e aplicação do art. 12.º n.º 1 alínea b) do MAR[336]. São indicadores não exaustivos, e cuja aplicação não é obrigatória. Estes, por sua vez, são aprofundados na secção 2 do Anexo II do Regulamento Delegado 2016/522, por via do art. 4.º n.º 2 do mesmo regulamento, através de exemplos de práticas específicas e indicadores adicionais, que tipicamente preenchem o art. 12.º n.º 1 alínea b) do MAR. Como tal, se forem aplicáveis, um comportamento dificilmente não será considerado manipulação de mercado[337].

À semelhança da alínea a), esta alínea b) do n.º 1 do art. 12.º abrange as operações, a colocação de ordens e outras condutas. O conceito de «qualquer outra atividade ou conduta» foi concebido, à semelhança do que se verifica com a alínea a), com o objetivo de aumentar o escopo da alínea b) de modo a abranger o maior tipo de condutas manipulatórias, tentando, deste modo, evitar lacunas na norma e conferir o maior grau de proteção[338]. Em termos de conteúdo cobre também o mesmo tipo de condutas da alínea a). São, portanto, abrangidos quaisquer comportamentos ou condutas que violem a norma, nomeadamente por omissão[339]. O escopo da alínea b) é assim tão largo que abrange manipulações à base da informação e à base da negociação[340].

---

334 Art. 12.º n.º 1 alínea b) do do Regulamento (UE) n.º. 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

335 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 560.

336 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 563.

337 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 564.

338 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 561.

339 Ibid.

340 Ibid.

Para a manipulação de mercado da alínea em questão, os comportamentos devem ser acompanhados de procedimentos fictícios, ou outras formas de engano ou artifício. O conceito de artifício descreve comportamentos objetivamente adequados a enganar um investidor razoável acerca das verdadeiras circunstâncias económicas, especialmente acerca da oferta e procura de um instrumento financeiro[341].

Mais uma vez, à semelhança do que se verifica com as alíneas a) e c), o legislador europeu não exige que um determinado efeito se verifique, bastando-se com um certo grau de probabilidade[342] de um determinado comportamento para produzir certo efeito. É mais uma manifestação da tentativa de proteger ao máximo o mecanismo de formação dos preços nos mercados financeiros, presente no regime europeu da manipulação de mercado[343]. A probabilidade verifica-se com o teste objetivo do investidor razoável, questionando-se se para este investidor tal efeito no preço seria de esperar[344].

A questão da avaliação de um concreto comportamento para provocar erro no investidor realiza-se através da figura do investidor razoável, que negocia de forma racional, está adequadamente informado e possui sentido crítico[345].

No âmbito da NCIRRS e da alínea b), pode ser questionado se tanto as publicações nas redes sociais como a efetiva negociação coordenada levada a cabo pelos investidores de retalho utilizam algum tipo de engenho artificioso, que engane ou seja capaz de enganar um investidor razoável quanto a um instrumento financeiro.

A verificação da utilização de engenhos artificiosos na NCIRRS poderia dar-se pela divulgação de publicações nas redes sociais sobre instrumentos financeiros que estão na posse dos publicadores. No entanto, a nosso ver, tal prática não é compatível com o conceito de NCIRRS aqui analisado. Neste caso, alguém na posse de um instrumento financeiro divulga informações ou opiniões com o objetivo de, em seguida, aproveitar o efeito de subida ou queda do preço para negociar e obter lucro financeiro. Tal caso configura, ao invés, a prática de *scalping*[346]. Neste caso, a pessoa que divulga a informação sobre o instrumento financeiro que possui pretende aproveitar o movimento nos preços provocado por aquela divulgação para obter lucros financeiros. Distingue-se, portanto, da NCIRRS, no sentido em que as pessoas referidas não estariam a coordenar ou a dar instruções para a obtenção de um objetivo coletivo de influência sobre o preço, mas sim a aproveitar-se daquela divulgação de informação para obter lucros próprios. No entanto, práticas como a de *scalping* podem aparecer associadas à NCIRRS,

---

341 Klaus Schmolke, in: Lars Klöhn, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018, p. 562.

342 Na versão inglesa do MAR é usada a expressão "is likely". Ver nota de rodapé 200.

343 Ibid.

344 Ibid.

345 Ibid.

346 Também estabelecido diretamente no art. 12.º n.º 2 alínea d) do MAR.

tentando aproveitar-se desta. Neste caso tratar-se-ia de uma utilização da NCIRRS e não de um engenho artificioso colocado em prática pelos participantes no âmbito da estratégia coletiva.

7. CONCLUSÃO

Com esta dissertação pretendemos analisar a NCIRRS, percebendo se estas práticas são compatíveis com as características e os princípios de bons mercados financeiros defendidos pelo Direito e com as normas de manipulação de mercado vigentes na União Europeia.

Verificamos que os reguladores europeus pretendem mercados financeiros eficientes e proteger os investidores, e que, para tal, se pretendem bons mercados financeiros, os quais assentam nas características de eficiência, liquidez e estabilidade (volatilidade baixa).

Comparámos a NCIRRS com o conceito clássico da manipulação de mercado fornecida pelo caso norte-americano *Cargill v. Hardin*, do qual resulta a coincidência de práticas que de forma intencional influenciam o preço de mercado de modo a que este não mais espelhe a interação das forças de procura e oferta. Da comparação das consequências da manipulação de mercado com as consequências verificadas e previsíveis da NCIRRS resulta também uma coincidência de ambas. Assim, também a NCIRRS pode provocar a falha dos preços em refletir a informação disponível sobre os ganhos subjacentes, bem como toda a informação relevante disponível, e consequente perigo de falha de alocação de recursos nos mercados financeiros (ineficiência alocativa e informativa). Pode ainda levar à diminuição da confiança nos mercados financeiros (ineficiência institucional), e ao possível afastamento de mecanismos de ajustamento do preço, como as vendas a descoberto. Em casos extremos pode ter o mesmo destino do mercado de limões de Akerlof – o gradual abandono dos mercados, a perda de liquidez e o aumento da volatilidade e diminuição da estabilidade. Finalmente, de uma cumulação das consequências referidas pode a economia sofrer com as dificuldades das empresas e a diminuição dos postos de trabalho.

Daqui, concluímos que a NCIRRS, produzindo efeitos semelhantes aos do conceito tradicional de manipulação de mercado, prejudica a eficiência, liquidez e estabilidade dos mercados financeiros. Sendo estas características próprias de mercados financeiros eficientes, que constituem o objetivo dos reguladores europeus e que o Direito prossegue, então a NCIRRS é contrária aos objetivos da regulação dos mercados financeiros.

De seguida, analisámos a possibilidade de submissão da NCIRRS ao artigo 12.º do MAR, com especial foco nos casos GME e das "ações *meme*". Começamos pela análise da efetiva negociação coordenada concretizada

pelos investidores de retalho à luz da alínea a) do número 1 e alínea a) do número 2 do MAR.

Começando pelo art. 12.º n.º 1 alínea a) i) do MAR, concluímos que a conduta de negociação dos investidores de retalho pode produzir efeitos consideráveis no preço de um instrumento financeiro, nomeadamente sob a forma de informações relativas ao preço e à procura do referido instrumento, que, por sua vez, na medida em que contrariam a realidade, dão indicações falsas ou enganosas relativas ao referido instrumento. Sendo consideráveis os efeitos no preço, um investidor razoável provavelmente tomará as indicações falsas ou enganosas em conta para a tomada da sua decisão de investimento.

Já na secção ii) da alínea a) do n.º 1 do mesmo artigo, verificamos que a efetiva negociação coordenada pode influenciar o preço de um instrumento financeiro, adulterando o mecanismo da sua formação e afastando-o do seu valor fundamental.

Quanto à alínea a) do n.º 2 do art. 12.º do MAR, interpretada extensivamente, estabelecemos que a NCIRRS do caso GME obteve uma posição dominante, exercendo uma influência abusiva, uma vez que através da negociação de ações da GME e de instrumentos derivados, cujo ativo base são as ações da GME, influenciou os preços intencionalmente, e de forma significativa, distorcendo-os (afastando-os dos seus valores fundamentais) e gerando, deste modo, condições não equitativas que levaram ao *short squeeze* de partes com posições de venda a descoberto. Tal demonstra o potencial da NCIRRS de obtenção de tais efeitos.

No entanto, dificilmente se poderão aplicar as secções i) e ii) da alínea a) do n.º 1 e a alínea a) do n.º 2 do art. 12.º do MAR, uma vez que estas esbarrarão no requisito da conexão entre os investidores de retalho. O facto de a negociação de cada investidor de retalho participante individualmente não ter aptidão para influenciar os preços e cumprir os requisitos nem da secção i) nem da secção ii) da alínea a) do n.º 1 do art. 12.º do MAR, faz com que o requisito de conexão seja essencial na ponderação da aplicação desta alínea. Apesar de as redes sociais permitirem a participação de um grande número de investidores de retalho, cujo volume de negociação é comparável à de um grande investidor institucional, e sendo os potenciais efeitos da NCIRRS inegáveis, estes podem encontrar-se espalhados por diversos países e ordenamentos jurídicos, comportando a investigação da participação custos enormíssimos. Para além disso, não é clara a existência de um método eficaz a utilizar para determinar quais os investidores de retalho participantes, uma vez que estes não estão ligados por obrigações mútuas de execução da estratégia, que a maior parte destes não declara expressamente a sua participação e que se podem verificar comportamentos negociais semelhantes às suas sem a participação na negociação coordenada. Por esta razão, dificilmente se poderão aplicar, sem mais, as alíneas a) do n.º 1 e a) do n.º 2 do art. 12.º do MAR.

Por último, analisamos as publicações nas redes sociais no âmbito da negociação coordenada de investidores de retalho em relação às alíneas b) e c) do n.º 1 do art. 12.º do MAR.

Concluímos que a primeira parte do art. 12.º n.º 1 alínea c) do MAR não se aplica às publicações nas redes sociais no âmbito da NCIRRS, visto que as indicações falsas ou enganosas por elas dadas não serão tomadas em consideração por um investidor razoável, apesar de se verificar o requisito subjetivo e de poderem transmitir informação. Este investidor não tomará em conta, na sua decisão de investimento, indicações provenientes de utilizadores de redes sociais, na sua maioria sem possibilidade de verificação da identidade e da fiabilidade dos conhecimentos dos mesmos.

Por outro lado, a segunda parte do art. 12.º n.º 1 alínea c) do MAR é a nosso ver aplicável, podendo as publicações no âmbito da NCIRRS transmitir informação que levará intencionalmente os preços a atingirem níveis artificiais e anormais, desviando-se dos seus valores fundamentais e da normal interação entre as forças da procura e oferta. Em relação à efetiva negociação coordenada enquanto manipulação de mercado à luz do art. 12.º n.º 1 alínea a) do MAR, cuja aplicação poderá esbarrar no requisito de conexão entre os numerosos participantes da NCIRRS, a aplicação da alínea c) às publicações apresenta a vantagem de estas serem realizadas por uma pessoa e pelo facto de esta conduta de forma individual já poder preencher os requisitos. Como tal, esta não padece dos problemas que surgem do número de participantes, nomeadamente a investigação e o número de diferentes países e ordenamentos jurídicos que poderão estar envolvidos. Deste modo, as publicações que dão início e coordenam a NCIRRS podem ser consideradas como manipulação do mercado, violando a proibição da prática ou tentativa de manipulação de mercado do artigo 15.º do MAR.

Por último, a alínea b) do n.º 1 do art. 12.º do MAR não encontra aplicação na NCIRRS, visto que neste conceito de negociação os investidores de retalho discutem e publicam instruções nas redes sociais para a efetivação da estratégia pelo coletivo, e não para individualmente tirarem lucros financeiros dos efeitos da divulgação das informações, não se manifestando aqui, assim, a existência de procedimentos fictícios ou outras formas de engano ou artifício. No entanto, práticas como as de *scalping* podem aparecer associadas à NCIRRS tentando aproveitar-se desta, tratando-se neste caso de uma utilização da NCIRRS e não de um engenho artificioso colocado em prática pelos participantes no âmbito da estratégia coletiva.

Retiramos, finalmente, as seguintes respostas aos problemas a que nos propusemos responder:

(1) A NCIRRS tem o potencial para produzir efeitos semelhantes aos da tradicional manipulação de mercado, contrariando os objetivos da regulação dos mercados financeiros e o conceito de bons mercados que o Direito procura proteger, bem como para diminuir a eficiência, reduzir a liquidez e aumentar a volatilidade e a instabilidade dos mercados, prejudicando a

função dos mercados e diminuindo a confiança dos investidores nestes. O maior fator de distinção entre a NCIRRS e a tradicional manipulação de mercado é o facto de a conduta negocial individual dos investidores de retalho não ser apta a produzir uma influência considerável nos preços, apenas o sendo a conduta negocial dos investidores de retalho participantes enquanto coletivo.

(2) O MAR é aplicável à NCIRRS, mas apenas de forma muito limitada. Apenas as publicações que coordenam a negociação coletiva poderão preencher o artigo 12.º, e consequentemente violar a proibição do artigo 15.º do MAR. A falha de aplicação do MAR à efetiva negociação coordenada dos investidores de retalho, pela dificuldade da verificação do requisito da conexão dos investidores, sublinha a novidade desta prática e o problema colocado pelo referido grande fator de distinção entre estas e a manipulação de mercado, nomeadamente a distinção entre investidores de retalho envolvidos e não envolvidos. Nem mesmo um artigo de critérios amplos e de conceitos abertos, como é o 12.º do MAR, apresenta capacidade de aplicação à NCIRRS, sendo apenas aplicável às publicações que coordenam a efetiva negociação dos investidores de retalho envolvidos. Tal é problemático, uma vez que apenas se poderá aplicar a punição aos publicadores das instruções nas redes sociais, deixando de fora o grande número de pessoas envolvidas que executam a estratégia.

Será para o futuro importante proceder a estudos no sentido de perceber o grau de sucesso do regime europeu da manipulação de mercado em punir as publicações que instruem a NCIRRS, especialmente atendendo ao grau de anonimidade que se verifica, e se tal diminui a probabilidade de ocorrência destas práticas. Tal será também importante no sentido de analisar a necessidade de atualizar este regime de modo a cobrir também a efetiva negociação coordenada dos investidores de retalho, assim como a existência de métodos eficazes de investigação da participação.

8. REFERÊNCIAS BIBLIOGRÁFICAS

Akerlof, George, "The Market for "Lemons": Quality Uncertainty and the Market Mechanism", *The Quarterly Journal of Economics*, Vol. 84, n.º 2, Oxford, Oxford University Press, 1970.

Allen, Franklin; e Gale, Douglas, "Stock-Price Manipulation", *Review of Financial Studies*, Vol. 5, n.º 3, 1992, pp. 503-529.

—; Litov, Lubomir; e Mei, Jianping, "Large Investors, Price Manipulation, and Limits to Arbitrage: An Anatomy of Market Corners", *Review of Finance*, Vol. 10, n.º 4, 2006, pp. 645-693.

—; *et al*., "Squeezing Shorts Through Social Media Platforms", *Swiss Finance Institute Paper n.º 21-31*, 2021. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://ssrn.com/abstract=3823151 >.

Alloway, Annie; e Massa; Tracey, *Robinhood's Role in the 'Gamification' of Investing - Bloomberg*, [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW: <URL: https://www.bloomberg.com/news/articles/2020-12.-19/robinhood-s--role-in-the-gamification-of-investing-quicktake >.

Almeida, Gonçalo, *Lembra-se da GameStop ou da AMC? As "meme stocks" continuam a dar que falar em Wall Street - Jornal de Negócios* [Em linha] [Consult. 21 jun. 2021]. Disponível em WWW:<URL: https://www.jornaldenegocios.pt/mercados/detalhe/lembra-se-da-gamestop-ou-da-amc-as-meme-stocks-continuam-a-dar-que-falar-em-wall-street >.

Anderson, John; Kidd, Jeremy; e Mocsary, George, "*Social Media, Securities Markets, and the Phenomenon of Expressive Trading"*, 2021. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://ssrn.com/abstract=3834801 >.

Armour, John; et al., *Principles of Financial Regulation*, 1ª edição, Oxford, Oxford University Press, 2015.

Assmann, Heinz-Dieter, *Prospekthaftung als Haftung für die Verletzung kapitalmarktbezogener Informationsverkehrspflichten nach deutschem und US-amerikanischem Recht*, Köln, Carl Heymanns Verlag, 1985.

Avgouleas, Emilios, *The Mechanics and Regulation of Market Abuse*, 1ª edição, Oxford, Oxford University Press, 2005.

Bayram, Milan, *Manipulative Handelspraktiken gemäß Art. 12. MAR*, 1ª edição, Berlin, Duncker & Hublot, 2020.

Bianco, Jim, *Wall Street Never Saw the Redditors Coming - Bloomberg* [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.bloomberg.com/opinion/articles/2021-02-02/wall-street-didn-t-see-reddit-s-wallstreetbets-coming-for-gamestop-gme >.

Bodie, Zvi; Kane, Alex; e Marcus, Alan, *Investments*, 11ª edição, New York, McGraw-Hill Education, 2018.

Buck-Heeb, Petra*, Kapitalmarktrecht*, 9ª edição, München, C.F. Müller, 2017.

Bumke, Christian, "Regulierung am Beispiel der Kapitalmärkte – Eine Untersuchung über Konzeption und Dogmatik des Regulierungsverwaltungsrechts" in: Hopt, Klaus, Veil, Rüdiger e Kämmerer, Jörn, *Kapitalmarktgesetzgebung im europäischen Binnenmarkt*, 1ª edição, Tübingen, Mohr Siebeck, 2008, pp. 107-142.

Câmara, Paulo, *Manual de direito dos valores mobiliários*, 4ª edição, Coimbra, Almedina, 2018.

Cordeiro, António Barreto Menezes, Manual de Direito dos Valores Mobiliários, 2ª edição, Coimbra, Almedina, 2019.

Costola, Michele and Iacopini, Matteo and Santagiustina, Carlo, "On the "mementum" of Meme Stocks", 2021. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://ssrn.com/abstract=3861779 >.

Cunningham, Lawrence, "Capital Market Theory, Mandatory Disclosure and Price Discovery", Washington and Lee Law Review, Vol. 51, n.º 3, 1994, pp.843-877.

Enriques, Luca; e Gatti, Matteo, "Is there a Uniform EU Securities Law After the Financial Services Action Plan?", *Stanford Journal of Law, Business and Finance*, Vol. 14, n.º 1, 2008.

Ensign, Rachel, *GameStop Investors Who Bet Big—and Lost Big - Wall Street Journal* [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.wsj.com/articles/gamestop-investors-who-bet-bigand-lost-big-11613385002 >.

Fama, Eugene, "Efficient Capital Market: A Review of Theory and Empirical Work", The *Journal of Finance*, Vol. 25, n.º 2, 1970, pp. 383-417.

—; e French, Kenneth, "The Capital Asset Pricing Model: Theory and Evidence", 2003. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://ssrn.com/abstract=440920 >.

Fischel, Daniel; e Ross, David, "Should Law Prohibit Manipulation?", Harvard Law Review, Vol.105, 1991, pp. 503-553

Friedman, Richard, "Stalking The Squeeze: Understanding Commodities Market Manipulation", *Michigan Law Review*, Vol. 89, 1990, pp. 30-68.

Gilson, Ronald; e Kraakman, Reinier, "The Mechanisms of Market Efficiency", *Virginia Law Review*, Vol.70, n.º 4, 1984, pp. 549-644.

Greifeld, Katherine; e Wang, L, *GameStop Short Interest Plunges in Sign Traders Are Covering - Bloomberg* [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.bloomberg.com/news/articles/2021-02-01/games-top-short-interest-plummets-in-a-sign-traders-are-covering >.

Guggenberger, Elena in Kalss, Susanne *et al*., *EU Market Abuse Regulation: A Commentary on Regulation (EU) No 594/2014*, 1ª edição, Cheltenham, Edward Elgar Publishing. 2021.

Harris, Larry, *Trading & Exchanges*, 1ª edição, Oxford, Oxford University Press, 2002.

Javers, Eamo, *Republicans in Washington warn Wall Street: The GameStop Populists Are More Powerful than You Think - CNBC* [Em linha] [Consult. 21 jun. 2022]. [Em linha] [Consult. 21 jun. 2021]. Disponível em WWW:<URL: https://www.cnbc.com/2021/01/28/gamestop-republicans-warn-of-trump-style-populist-revolution.html >.

Kahan, Marcel, "Securities Laws and the Social Costs of Inaccurate Stock Prices", *Duke Law Journal*, Vol. 41, 1992, pp. 977-1044. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://scholarship.law.duke.edu/dlj/vol41/iss5/1 >.

Keatinge, Colin - *Melvin Lost 53% in January, Hurt by GameStop, Other Bets – Bloomberg* [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.bloomberg.com/news/articles/2021-01-31/melvin-lost-53-in-january-hurt-by-gamestop-other-bets-dj >.

Kharif, Olga - *What's the $23 Billion GameStop Really Worth? Maybe $2 Billion - Bloomberg* [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.bloomberg.com/news/articles/2021-01-27/what-s-the-23-billion-gamestop-really-worth-maybe-2-billion >.

Klöhn, Lars, *Kapitalmarkt, Spekulation und Behavioral Finance*, Berlin, Duncker & Hublot, 2006.

—; "Kapitalmarktrecht" *in* Langenbucher, Katja, 4ª edição, *Europäisches Privat- und Wirtschaftsrecht*, Baden-Baden, Nomos, 2017.

Lev, Baruch e Villiers, Meiring de, "Stock Price Crashes and 10b-5 Damages: A Legal, Economic, and Policy Analysis", *Stanford Law Review*, Vol. 47, n.º 1, 1994, pp. 7-37.

Levine, Matt - *The Meme Stocks keep coming - Bloomberg* [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.bloomberg.com/opinion/articles/2021-06-09/the-meme-stocks-keep-coming >.

—, *The GameStop Game Never Stops - Bloomberg* [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.bloomberg.com/opinion/articles/2021-01-25/the-game-never-stops?sref=1kJVNqnU >.

Macey, Jonathan; *et al.,* "Lessons from Financial Economics: Materiality, Reliance, and Extending the Reach of Basic v. Levinson", *Virginia Law Review,* Vol. 77, 1991, pp. 1017-1049.

—, "Securities Regulation as Class Warfare", *Columbia Business Law Review*, 2021. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://ssrn.com/abstract=3789706 >.

Mannweiler, Antonia - *Hashtag #Marktmanipulation - Frankfurter Allgemeine Zeitung*, [Em linha] [Consult. 06 jun. 2022]. Disponível em WWW:<URL: https://www.faz.net/aktuell/finanzen/aktienmarkt-und-social-media-verdacht-auf-marktmanipulation-17570647.html >.

McVea, Harry, "Supporting Market Integrity" in Moloney, Niamh, Ferran, Eilís e Payne, Jennifer, *The Oxford Handbook of Financial Regulation,* 1ª edição, Oxford, Oxford University Press, 2015, pp. 631-658.

Merwald, Maximilian; e Schauer, Pirmin, "Marktmanipulation, Social Media und Noise Trader im Fall GameStop", *BKR*, 2021, p. 280-292.

Miller, Edward, "Risk, Uncertainty and Divergence of Opinion", *The Journal of Finance,* Vol. 32, n.º 4, 1977, pp. 1151-1168.

Mitts, Joshua; *et al*., *A Report by the Ad Hoc Academic Committee on Equity and Options Market Structure Conditions in Early 2021*, 2022, [Em linha] [Consult. 17 de junho de 2022]. Disponível em WWW:<URL: https://ssrn.com/abstract=4030179 >.

Moloney, Niamh, *EU Securities and financial markets regulation*, 3ª edição, Oxford, Oxford University Press, 2016.

Mülbert, Peter, "Art. 12. VO Nr. 596/2014", in: Heinz-Dieter Assmann, Uwe Schneider e Peter Mülbert, *Wertpapierhandelsrecht*, 7ª edição, Köln, Otto Schmidt, 2019.

Nagarajan, Shalini - *GameStop explodes another 157% higher after Elon Musk's 'Gamestonk' tweet extends Reddit-driven short squeeze - Business Insider*, [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://markets.businessinsider.com/news/stocks/gamestop-stock-price-elon-musk-gamestonk-tweet-extends-trading-rally-2021-1-1030009065 >.

Otte, Jedidajah - *Sending a Message': GameStop Investors on Why They Boaught Shares - The Guardian* [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.theguardian.com/business/2021/jan/28/sending-a-message-gamestop-investors-on-why-they-bought-shares >.

Pedersen, Lasse, *Game On: Social Networks and Markets*, NYU Stern School of Business, 2021. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://ssrn.com/abstract=3794616 >.

Pensions & Investments. [Em linha] [Consult. 29 de abril de 2022]. Disponível em WWW:<URL: https://www.pionline.com/article/20170425/INTERACTIVE/170429926/80-of-equity-market-cap-held-by-institutions >.

Perdue, Wendy, 'Manipulation of Futures Markets: Redefining the Offense', *Fordham Law Review*, Vol. 56, n.º 3, 1987, pp. 345-402.

Phillip, Matt; *et al*. - *The Hopes That Rose And Fell With GameStop" - New York Times* [Em linha] [Consult. 11 de abril de 2022]. Disponível em WWW:<URL: https://www.nytimes.com/2021/02/07/business/gamestop-stock-losses.html >.

Pinto, Frederico Costa, *O Novo Regime dos Crimes e Contra-Ordenações no Código dos Valores Mobiliários,* 1ª edição, Coimbra, Almedina, 2000.

Poelzig, Dörte, *Kapitalmarktrecht*, 2ª edição, München, C.H. Beck, 2021.

Robertson, Harry - *Short-Sellers Are Nursing Estimated Losses Of $19 Billion in 2021 After Betting on GameStop's Stock to Plunge - Business Insider* [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://markets.businessinsider.com/news/stocks/short-sellers-sitting-on-19-billion-of-losses-on-GameStop-data-shows-2021-1-1030020684 >.

Robinson, Matt, *Meme-Stock Frenzy Gets a Fresh Look That Questions SEC Narrative - Bloomberg*, [Em linha] [Consult. 17 de junho de 2022]. Disponível em WWW:<URL: https://www.bloomberg.com/news/articles/2022-02-14/meme-stock-frenzy-gets-a-fresh-look-that-questions-sec-narrative >.

Roseiro, Duarte, As sociedades de notação de risco e o crime de manipulação do mercado, 2017. [Em linha] [Consult. 17 de junho de 2022]. Disponível em WWW:<URL: https://run.unl.pt/handle/10362/20346 >.

Sajnovits, Alexander, "GameStop im Lichte der MAR – Meme-Trading, soziale Medien und Handelsbeschränkungen durch Broker", *Zeitschrift für Unternehmens- und Gesellschaftsrecht*, vol. 50, n.º 5, 2021, p. 810 (pp. 804–845).

Sarr, Abdourahmane; e Lybek, Tonny, "Measuring Liquidity in Financial Markets", *IMF Working Paper*, 2002. [Em linha] [Consult. 17 de junho de 2022]. Disponível em WWW:<URL: https://www.elibrary.imf.org/view/journals/001/2002/232/article-A001-en.xml >.

Schmolke, Klaus in: Klöhn, Lars, *Marktmissbrauchsverordnung: MAR*, 1ª edição, München, C.H. Beck, 2018.

Schröder, Christian, *Handbuch Kapitalmarktstrafrecht*, 3ª edição, Heymanns Verlag GmbH, 2015.

Shiller, Robert, *Irrational Exuberance*, 3ª edição, Princeton University Press, 2016.

Silva, Miguel Moura E, *Direito da Concorrência*, 2ª edição, Lisboa, AAFDL Editora, 2018, pp. 883 e ss.

Stout, Lynn, "The Mechanisms of Market Inefficiency: An Introduction to the New Finance", 2003, [Em linha] [Consult. 17 de junho de 2022]. Disponível em WWW:<URL: https://ssrn.com/abstract=470161>.

Teigelack, Lars, "Market Manipulation" *in* Veil, Rüdiger, *European Capital Markets Law*, 2ª edição, Oxford, Hart Publishing, 2017, pp 225 a 259.

Veiga, Alexandre Brandão da, *Crime de Manipulação, Defesa e Criação de Mercado*, 1ª edição, Coimbra, Almedina, 2001.

Veil, Rüdiger, "Europäisches Insiderrecht 2.0 – Konzeption und Grundsatzfragen der Reform durch MAR und CRIM-MAD", *Zeitschrift für Bankrecht und Bankwirtschaft*, 2014

—; e Templer, Lena, "GameStop, Reddit und die Hedgefonds - Betrachtungen aus der Perspektive des europäischen Kapitalmarktrechts", *ZIP*, 2021.

Ventoruzzo, Marc; e Mock, Sebastian, *Market Abuse Regulation Commentary and Annotated Guide*, 1ª edição, Oxford, Oxford University Press, 2017.

Verlaine, Julia-Ambra; e Banerji, Gunjan - *Keith Gill Drove the GameStop Reddit Mania. He Talked to the Journal - Wall Street Journal* [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW: <URL: https://www.wsj.com/articles/keith-gill-drove-the-GameStop-reddit-mania-he-talked-to-the-journal-11611931696 >.

Warren. Elizabeth, Letter to the Acting Chair of the U.S. Securities and Exchange Commission (SEC). United States Senate, 2021. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.warren.senate.gov/imo/media/doc/01.29.2021%20Letter%20from%20Senator%20Warren%20to%20Acting%20Chair%20Lee.pdf >.

Wegner, Kilian, "Das „GameStop"-Phänomen nach deutschem Marktmissbrauchsrecht:Marktmanipulation oder legitimes Anlegerverhalten?", *BKR*, 2021, pp. 181-188.

LEGISLAÇÃO EUROPEIA

Regulamento (UE) n.º 596/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014.

Regulamento Delegado 2016/522

Regulamento (UE) n.º 236/2012. do Parlamento Europeu e do Conselho de 14 de março de 2012.

Diretiva 2014/65/UE do Parlamento Europeu e do Conselho de 15 de maio de 2014

Tratado de Funcionamento da União Europeia

Diretiva 2004/109/CE do Parlamento Europeu e do Conselho de 15 de dezembro de 2004.

EUROPEAN SECURITIES AND MARKETS AUTHORITY

ESMA, ESMA's technical advice on possible delegated acts concerning the Market Abuse Regulation, ESMA/2015/224, 3 de fevereiro de 2015, p. 78. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.esma.europa.eu/document/esma%E2%80%99s-technical-advice-possible-delegated-acts-concerning-market-abuse-regulation >.

ESMA, Final Report, Draft Technical standards on the Market Abuse Regulation, 28 de setembro de 2015, ESMA/2015/1455, p. 72. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.esma.europa.eu/sites/default/files/library/2015/11/2015-esma-1455_-_final_report_mar_ts.pdf >.

FINANCIAL CONDUCT AUTHORITY

Financial Conduct Authority (2016) *FCA Handbook* MAR. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.handbook.fca.org.uk/handbook/MAR/1/?view=chapter >.

IOSCO

IOSCO - Technical Committee of the International Organization of Securities Commissions, 'Investigating and Prosecuting Market Manipulation', Maio de 2000 [Em linha] [Consult. 21 jun. 2021]. [Em linha] [Consult. 21 jun. 2021]. Disponível em WWW:<URL: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD103.pdf >.

IOSCO, 2000 IOSCO Market Manipulation Report, n.º 34. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD103.pdf >.

IOSCO, Investigating and Prosecuting Market Manipulation, maio de 2000. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD103.pdf >.

RESERVA FEDERAL AMERICANA

Board of Governors of the Federal Reserve System, Financial Stability Report, novembro de 2021, p. 18 a 21. [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://www.federalreserve.gov/publications/files/financial-stability-report-20211108.pdf >.

JURISPRUDÊNCIA

Cargill, Inc v Hardin 452 F 2d 1154, 1164–65 (8th Cir 1971)

TJUE, 7.7.2011, Processo C-445/09 – (IMC Securities), ECLI:EU:C:2011:459, [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0445 >.

COMUNICAÇÃO DA COMISSÃO

Comunicação da Comissão, Orientação sobre as prioridades da Comissão na aplicação do artigo 82.º do Tratado CE a comportamentos de exclusão abusivos por parte de empresas em posição dominante, [Em linha] [Consult. 21 jun. 2022]. Disponível em WWW:<URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:045:0007:0020:PT:PDF >.

REGULAÇÃO DA CRIPTOECONOMIA: SITUAÇÃO ATUAL E SUPERAÇÃO DO PARADIGMA TRADICIONAL DE SOBERANIA

Rômulo Pinto de Lacerda Santana

romuloplsantana@gmail.com

Resumo: Este estudo tem como objetivo verificar se as regulações estatais de cunho nacional para o mercado de criptoativos são capazes de, isoladamente, proporcionar segurança jurídica e operacional, ao mesmo tempo propiciando ambiente saudável a todos os envolvidos e que não sufoque o potencial inovador do setor. Para tanto, foi identificado o contexto histórico de surgimento do *bitcoin* enquanto primeiro criptoativo e a evolução da tecnologia *blockchain*, que possibilitou a multiplicidade de aplicações nesta nova economia, identificando-se problemas relacionados à utilização destes ativos para fins criminosos, tributação dessas manifestações de riqueza, captação pública de valores e a necessária proteção dos investidores, higidez do sistema financeiro e monetário, e sustentabilidade socioambiental. Assim, fez-se de início revisão da literatura sobre a temática e análise sobre o estágio de regulação da criptoeconomia no cenário internacional, sendo identificados entendimentos díspares e por vezes opostos, limitação de aplicabilidade pela territorialidade e diferenças relevantes na evolução da regulação em cada Estado soberano. Por sua vez, inserida a realidade dentro da economia digital, em cenário de globalização jamais antes experimentado, verificam-se propostas e iniciativas policêntricas, com foco na necessária visão mundial do fenômeno, com fim de padronização das normas e regras existentes. Chega-se à conclusão de que o paradigma tradicional de soberania se encontra nesta seara ultra-

passado, tendo em vista a criptoeconomia estar inserida em realidade que tem potencial de atingir instantaneamente todo o ambiente internacional, o que deve ensejar medidas colaborativas que não se restrinjam a limites territoriais específicos. Com isso, objetiva-se gerar segurança jurídica aos operadores econômicos, eficiência e certeza às administrações fiscais, estabilidade financeira no desenvolvimento dos serviços prestados, e evitar o cometimento de ilícitos ao se dificultar a atuação do agente em face da pretensa redução do problema de deslocamento para jurisdições menos exigentes. Trata-se, em síntese, de pesquisa dogmática ou instrumental, com importante viés sociojurídico. Utilizam-se métodos de procedimento histórico, interpretativo e comparativo. O tipo de pesquisa se inicia como exploratória e descritiva, passando à explicativa diante da complexidade da matéria envolvida. O método de pesquisa é bibliográfico e documental. O tipo de pesquisa é de coleta e de análise de dados. O método de abordagem é primordialmente por dedução, ainda que se utilize da indução diante da compreensão do Direito enquanto fato social, bem como se utilize de premissa criminológica e de análise estatística do fenômeno para melhor compreendê-lo. Enquanto restrição metodológica, registra-se que o estudo não tem cunho empírico, experimental, de estudo de caso ou de campo, mas de interpretação dos dados obtidos a partir da literatura, dos entes estatais que atuam de forma soberana e ainda dos organismos internacionais inseridos no auxílio regulatório da matéria.

Palavras-chave: Criptoativos; Criptomoedas; Segurança Jurídica; Eficiência Fiscal; Estabilidade Econômica.

Abstract: This study aims to verify whether state regulations of a national nature for the crypto market are capable of, in isolation, providing legal and operational security, at the same time providing a healthy environment for all involved and that does not stifle the innovative potential of the sector. For this, the historical context of the emergence of bitcoin as the first crypto asset and the evolution of blockchain technology were identified, which enabled the multitude of applications in this new economy, identifying problems related to the use of these assets for criminal purposes, taxation of these manifestations of wealth, public raising of values and the necessary protection of investors, soundness of the financial and monetary system, and socio-environmental sustainability. Thus, a review of the literature on the subject and analysis of the stage of regulation of cryptoeconomics in the international scenario were carried out, identifying disparate and sometimes opposing understandings, limitation of applicability due to territoriality and relevant differences in the evolution of regulation in each State sovereign. In turn, inserting reality within the digital economy, in a scenario of globalization never experienced before, polycentric proposals and initiatives are verified, focusing on the necessary world view of the phenomenon, with the aim of standardizing existing norms and rules. It comes to the conclusion that the traditional paradigm of sovereignty is outdated in this area, considering that the cryptoeconomy is inserted in a reality that has the potential to instantly reach the entire international environment, which should give rise to collaborative measures that are not restricted to limits specific territories. With this, the objective is to generate legal certainty for economic operators, efficiency and certainty

for tax administrations, financial stability in the development of services provided, and to avoid the commission of illicit acts by making it difficult for the agent to act in view of the alleged reduction of the displacement problem for less demanding jurisdictions. It is, in summary, dogmatic or instrumental research, with an important socio-legal bias. Methods of historical, interpretative and comparative procedure are used. The type of research begins as exploratory and descriptive, moving on to explanatory in view of the complexity of the matter involved. The research method is bibliographical and documental. The type of research is data collection and analysis. The method of approach is primarily by deduction, even if it uses induction in the face of understanding Law as a social fact, as well as using a criminological premise and statistical analysis of the phenomenon to better understand it. As a methodological restriction, it is noted that the study does not have an empirical, experimental, case study or field nature, but rather an interpretation of data obtained from the literature, from state entities that act in a sovereign way and even from international organizations inserted in the regulatory assistance of the matter.

Keywords: Cryptoassets; Cryptocurrencies; Legal Certainty; Fiscal Efficiency; Economic Stability.

1. INTRODUÇÃO

No estágio de evolução societária atual, em um período de globalização intensa de serviços, pessoas, bens e capitais, há necessidade de superação da tradicional tutela dos direitos individualizados, dando primazia à realidade da tutela de direitos de natureza transindividual. No sentido de delimitar a importância e objeto deste trabalho, ciente do processo de digitalização do dinheiro, com utilização de cartões de crédito, cartões de débito e moedas eletrônicas, dentro do contexto de *e-commerce* que influencia a economia digital, verifica-se que todas estas alternativas estão ligadas às moedas oficialmente emitidas por Estados. Por isso, o presente estudo se direciona ao surgimento do *bitcoin* enquanto primeiro criptoativo existente, movimento cunhado na promessa de revolucionar o sistema financeiro.

Assim, com a sociedade de massa, que não respeita a fronteira entre os diversos Estados, surgem questões que necessitam de análises cooperativas e regulatórias para atingirem a sua resolução, em que a criptoeconomia[1] é uma das mais atuais e relevantes. Leve-se em conta as várias atividades inseridas e a multilocalização dos *players* envolvidos, o que é acompanhado pela diversidade de entidades, órgãos e organismos, nacionais e internacionais, que almejam a compreensão e regulação dos negócios jurídicos inerentes.

Neste contexto, diante das cifras bilionárias que são diariamente comercializadas dentro do mercado de criptoativos[2] espalhado em todo o mundo, tentam, de alguma forma, lançar mão de princípios, classificações e entendimentos sobre as diversas operações englobadas e não inteiramente regulamentadas, seja através de instruções, legislações ou regulamentos, causando tratamentos díspares e até contraditórios ao complexo fenômeno em exame, inclusive sobre a natureza jurídica dos negócios apreciados.

Desse modo, considerando a utilidade e oportunidade de discussão sobre o tema, este trabalho se orienta em sentido diferente do que vem usualmente sendo objeto de estudo, ao se direcionar a uma análise holística e, portanto, não direcionada ou inserida em apenas um ordenamento jurídico. Por isso, possui como objeto geral e delimitado compreender e refletir se as regulações puramente nacionais, consubstanciadas no paradigma tradicio-

[1] Não se resumindo às criptomoedas, ciente das discussões acerca da classificação dos ativos envolvidos, que não será objeto de conclusão neste trabalho, entende-se como criptoeconomia todas as atividades jurídico-econômicas dos *tokens* enquanto representações digitais e criptografadas de ativos, sejam nativos do meio digital (criptoativos) ou objeto de *tokenização* de ativos físicos. Conforme classificação mais comumente utilizada, podem ser *tokens* de pagamento, de utilidade ou de valores mobiliários, muito embora estejamos diante de novas espécies, a exemplo dos *tokens* não fungíveis ou NFT e os que se relacionam às intituladas finanças descentralizadas ou DeFi.

[2] Registre-se desde já que os termos *criptoativos* e *criptomoedas* não são utilizados como sinônimos, tendo em vista que o primeiro é gênero do qual o segundo é apenas uma de suas espécies.

nal de soberania, configuram-se como bastantes para desenvolver ambiente seguro e operacional, propiciando ambiente saudável e que não sufoque o potencial inovador do setor.

Como objetivos específicos, os quais têm o condão de representar cada capítulo deste trabalho, verifica-se a necessidade de (1) comprovar expressamente a importância da criptoeconomia no ambiente de globalização atual, bem como da tecnologia *blockchain* que lhe é subjacente; (2) identificar os principais problemas verificados neste comércio de criptoativos; (3) explicitar a situação regulatória atual nos principais países em termos de importância e amadurecimento no setor, incluindo Brasil e Portugal; e (4) descrever de forma sucinta como alguns organismos internacionais vêm auxiliando os Estados nacionais a devidamente enfrentarem a temática, passando-se às (5) conclusões do cenário observado.

Orienta-se como hipótese de pesquisa a necessidade de superação do paradigma tradicional de soberania, diante da complexidade do tema, que gera entendimentos contraditórios entre os órgãos nacionais dos Estados envolvidos, os quais não são competentes sozinhos para sanar ou ao menos evitar os problemas identificados, os quais têm potencial de atingir indistinta e instantaneamente qualquer país localizado no globo, circunstância esta jamais vivenciada nesse grau de incidência[3]. Diante da análise do fenômeno de forma holística, este trabalho servirá como perspectiva descritiva da complexidade dos problemas a serem enfrentados.

Assim, far-se-á pesquisa dogmática ou instrumental, com importante viés sócio-jurídico, utilizando-se do método de procedimento histórico acerca do contexto de surgimento da *bitcoin*, bem como a evolução das atividades relacionadas à tecnologia *blockchain*, ao passo que os procedimentos interpretativo e comparativo servirão para analisar o conteúdo de alguns dispositivos legais correlatos à temática, nacionais e internacionais, verificando-se a diferenciação de tratamento sob alguns aspectos, passando à conclusão ao final apresentada.

O tipo de pesquisa é primordialmente exploratório e descritivo, embora também seja explicativo diante da complexidade da matéria envolvida. O método de pesquisa é bibliográfico e documental. O tipo de pesquisa é de coleta e de análise de dados. O método de abordagem é por dedução, ainda que se utilize da indução diante da compreensão do Direito enquanto fato social, bem como se utilize de premissa criminológica e de análise estatística do fenômeno para melhor compreendê-lo. Enquanto restrição metodo-

---

[3] Ciente do perigo de ser considerada *tese panorâmica*, na classificação de Umberto Eco, *Como se faz uma tese em Ciências Humanas*, 19ª ed., Trad. Ana Falcão Bastos e Luís Leitão, Lisboa, Editorial Presença, 2015, p. 39, faz-se um corte metodológico que evidencie a exequibilidade da investigação, sobremaneira para justificar a proposição veiculada, servindo como ponto de partida para trabalhos futuros com enfrentamento concreto de problemáticas reais, a exemplo da classificação dos criptoativos, obrigações dos operadores econômicos e tributação das atividades.

lógica, o estudo não tem cunho empírico, experimental, de estudo de caso ou de campo, mas de interpretação dos dados obtidos a partir da literatura, dos entes estatais que atuam de forma soberana e ainda dos organismos internacionais inseridos no auxílio regulatório da matéria.

2. IMPORTÂNCIA CONTEMPORÂNEA DA CRIPTOECONOMIA

2.1. BREVES CONSIDERAÇÕES DO CONTEXTO DE GLOBALIZAÇÃO

Conforme Aguillar[4], entende-se como Direito Econômico o direito das políticas públicas na economia, ou seja, o conjunto de normas e institutos jurídicos que permitem ao Estado exercer qualquer tipo de influência no comportamento dos agentes econômicos no ambiente de um Estado ou mesmo de vários países, até mesmo de forma regionalizada.

Desse modo, nota-se que, historicamente, o papel do Estado na economia oscilou de forma pendular, ora em um processo de defesa da intervenção mínima, como no Liberalismo Econômico propagandeado por Adam Smith, ora em um momento de intervenção do aparelhamento estatal na economia, a exemplo do Estado de Bem-estar Social, influenciado pelas propostas de John Maynard Keynes.

Em cada momento histórico-político, a atuação mais branda ou incisiva do Estado nos negócios particulares de seus concidadãos foi conjunturalmente planejada, com vistas ao desenvolvimento ou sobrevivência do próprio sistema capitalista, enquanto processo não apenas de acumulação econômica, mas uma forma de civilização.

Saliente-se o estágio de evolução atual dos Estados nacionais, em que houve uma diferenciação no modo de governança, do Estado Positivo ao Estado Regulador, conforme preconiza Majone[5], especificando a mudança de foco dos instrumentos da tributação e, por consequência, das despesas estatais, antes com maior foco no desenvolvimento de atividades pelo próprio ente estatal, para ter como norte atual a elaboração de normas regulamentadoras dos diversos segmentos econômicos.

O paradigma da redistribuição e estabilização econômica como funções principais do Estado Positivo dá espaço à correção das falhas de mercado do Estado Regulador; ao invés de alocações orçamentárias, a arena principal de conflito político se configura na revisão e controle da formulação de regras. Em resumo, verifica-se o deslocamento da responsabilização políti-

---

4 Fernando Herren Aguillar, *Direito Econômico: do direito nacional ao direito supranacional*, São Paulo, Atlas, 2006, p. 1.

5 Giandomenico Majone, "Do Estado Positivo ao Estado Regulador: causas e consequências da mudança no modo de governança", *In Regulação econômica e democracia: o debate europeu*, São Paulo, Singular, 2006, p. 14.

ca da máquina estatal na direção dos negócios econômicos, que passa da ingerência direta, como promotor da atividade econômica, para a indireta, através da formulação de regras e regulamentos da respectiva atividade, capitaneadas pelas agências reguladoras e executivas.

Acerca do conceito de soberania, em sua perspectiva tradicional, liga-se umbilicalmente à ideia de Estado nacional, que, nos dizeres de Carrazza[6], é a única instituição soberana, por deter a "competência das competências". Por isso, declina como soberania "a faculdade que, num dado ordenamento jurídico, aparece como suprema", concluindo ser a soberania inerente à própria natureza do Estado.

Para tanto, fundamenta seu entendimento no sentido de que a soberania é una, originária, indivisível e inalienável, fazendo, assim, distinções acerca dos Estados simples ou unitários, e as uniões de Estados, sejam através da constituição de Confederações, como no caso dos Estados Unidos da América, ou das Federações, como ocorre com o Brasil[7].

Todavia, guardada a importância da doutrina tradicional quanto à noção clássica de soberania, diante do desenvolvimento socioeconômico dos Estados e a necessidade, por um lado, de propiciar trocas comerciais, de informações e promover ambientes de livre circulação, sejam de serviços, pessoas, bens e capitais, e, por outro lado, desenvolver mecanismos de combate às ilicitudes perpetradas por grandes organizações internacionais, a soberania puramente estatal vem dando espaço a blocos regionais de poder, em que se destaca, pela longevidade, integração e êxito em suas políticas, o caso da União Europeia.

Afora a propalada livre circulação empreendida já há muito tempo no ambiente europeu, importante registrar que também no campo fiscal-tributário esta integração vem ganhando cada vez mais força, principalmente no estabelecimento de regras comuns contra as práticas de fraude e evasão fiscais, muito embora ainda com certa timidez acerca da necessária harmonização de regras e bases tributárias, diante da autonomia de decisão através da anacrônica regra de unanimidade em matéria de impostos.

Assim, Ribeiro[8] acertadamente entende que a visão clássica de soberania absoluta não se configura como a mais apropriada, passando ao plano supranacional e assumindo um plano de exercício paralelo e com vias de integração, concluindo pela mudança de fronteiras da soberania, de puramente territoriais para essencialmente funcionais.

---

6 Roque Antonio Carrazza, *Curso de Direito Constitucional Tributário*, São Paulo, Malheiros, 2013, p. 148.

7 Para maiores detalhes sobre o tema, v. Roque Antonio Carrazza, *Op. Cit.*, p. 148-161.

8 João Sérgio Ribeiro, *Direito Fiscal da União Europeia: tributação direta*, Coimbra, Almedina, 2019, p. 23.

Muito embora o sentido epistêmico de soberania possa ser considerado estável, enquanto autoridade política, a atribuição específica a um determinado Estado passa a dar lugar ao exercício conjunto de competências, incluindo a sua função jurídica, com objetivos e funções comuns a realizar, inclusive em seu plano fiscal, sem dúvidas o mais difícil de ser atingido. Aliás, a adesão a tais regras comuns também demonstra ser um exercício de soberania por parte dos Estados, pois com a vinculação aos tratados regionais expressaram sua concordância com tais condicionalismos.

Também Feio[9] demonstra a ponderação de analisar modernamente o conceito, através de uma teoria mais cosmopolita. Perpassa, para análise do governo econômico, os critérios clássicos quanto ao modo de exercício do poder para novas referências além do conceito de governo, quais sejam, governança e governação, em um verdadeiro fenômeno de descentralização e desconcentração do poder, com base nos ideais de responsabilidade, transparência, coerência, eficácia e eficiência.

Ainda em suas conclusões[10], destaca conceitos de adaptação, integração e *accountability* como fundamentais para legitimar os novos enquadramentos transnacionais do Estado de Direito Democrático enquanto exercício do poder político, que se demonstra mais complexo, partilhado, elástico e em constante processo de transformação. Com isso, o próprio poder tributário vai perdendo as suas características de absoluto através da cedência por parte dos Estados de elementos relevantes de sua soberania econômica.

Tal fenômeno se verifica em maior grau diante da emergência da economia digital, que, conforme Teixeira[11], desafia os princípios e técnicas fiscais fundamentais, exigindo refinamento e especialização na fiscalização e acompanhamento de atividades como comércio eletrônico, jogos *on-line* e, mais recentemente, o mercado dos criptoativos, em que o próprio conceito de estabelecimento estável ou sede e direção efetiva se encontram em descompasso com a realidade. Destaca-se desde já o seu entendimento atualizado, que se acompanha integralmente, acerca da necessidade de aprofundamento das trocas de informações entre Estados para melhorar a eficiência na fiscalização dos abusos e das fraudes fiscais, resultado do aceleramento histórico diante da globalização das economias e do impacto das novas tecnologias da informação[12].

Por fim, nota-se que o fenômeno da globalização também se verifica através da emergência de problemas transnacionais, em que se destacam os fenômenos ambientais, como o crescente aquecimento global, que acaba por atingir indistintamente todos os países pelo mundo e, como via de conse-

---

9 Diogo Nuno de Gouveia Feio, *O Governo, o Orçamento e os Impostos: Uma história interminável entre a União Europeia e a União Económica e Monetária*, [S. l.], Petrony, 2020, p. 282.

10 Para maiores detalhes, v. Diogo Nuno de Gouveia Feio, *Op. Cit,* pp. 377-387.

11 Glória Teixeira, *Manual de Direito Fiscal*, Coimbra, Almedina, 2019, p. 401.

12 Glória Teixeira, *Op. Cit*., p. 423.

quência, devem ser enfrentados de forma conjunta, com políticas públicas que ultrapassem as fronteiras nacionais.

Dessa forma, tem-se como premissa básica a regulação estatal como forma de atuação dos países em meio ao fenômeno da globalização[13], que não se prende às fronteiras entre os Estados, tampouco respeita a soberania destes, tanto em seu aspecto interno como externo, necessitando-se de cooperação internacional entre as regiões atingidas pela homogeneização dos mercados através da ingerência de grandes corporações transnacionais.

2.2. SURGIMENTO DO BITCOIN COMO PRIMEIRO CRIPTOATIVO

Há ainda que se entender o momento histórico de surgimento que motivou a criação do primeiro criptoativo[14], o *bitcoin*, através da apresentação, por Satoshi Nakamoto[15], do *whitepaper* intitulado "*Bitcoin: A Peer-to-Peer Electronic Cash System*"[16], datado de 31 de outubro de 2008, programado para existência de 21 (vinte e uma) milhões de unidades.

Afora toda a construção centenária acerca da utilização de moeda como meio de pagamento, unidade de conta e reserva de valor[17], funções desempenhadas pelas moedas tradicionais cunhadas pelos Estados nacionais e soberanos[18], evidenciam-se neste momento as profundas crises econômicas enfrentadas no início do século XX, principalmente a Crise de 1929, co-

---

13 Maria Luiza Pereira de Alencar Mayer Feitosa, *Paradigmas inconclusos: os contratos entre a autonomia privada, a regulação estatal e a globalização dos mercados,* Coimbra, Coimbra, 2007, p. 169.

14 Conforme adiante se verá, o *bitcoin* foi a primeira criptomoeda criada, que se insere em uma multiplicidade de outros criptoativos, gênero do qual se configura apenas como uma de suas espécies.

15 Em que pese nunca ter havido comprovação de sua existência, aparentemente se trata de um pseudônimo para o(s) verdadeiro(s) autor(es) do programa, provavelmente um grupo de programadores que se dedicaram ao seu desenvolvimento.

16 Em tradução livre, "Bitcoin: um sistema monetário eletrônico ponto a ponto (ou desintermediado)". Disponível em <https://bitcoin.org/bitcoin.pdf>, consult. 27.11.2021.

17 Conforme se verifica em Maria do Carmo Garcez Ghirardi, *Criptomoedas: aspectos jurídicos* [Em linha], São Paulo, Almedina Brasil, 2020, p. 24, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556270364/>, consult. 27.11.2021: "Dessa forma, considerando que a palavra moeda é utilizada em circunstâncias diversas, mas sempre ligadas ao meio de pagamento empregado em determinada transação, ao conjunto de notas bancárias e metal cunhado de determinado país, ou ainda a um complexo de bens, depósitos bancários, títulos de crédito entre outros, o conceito de moeda é geralmente considerado na dinâmica das funções que assume: meio de pagamento, unidade de valor e reserva de valor". De forma bastante objetiva, reserva de valor permite que o poder de compra se mantenha no tempo, meio de troca ou de pagamento permite a troca por bens e serviços, e unidade de conta serve como referencial entre a troca de bens e serviços.

18 Para maiores detalhes, v. Maria do Carmo Garcez Ghirardi, *Op. Cit*., pp. 27-34 e Tarcísio Teixeira, *Direito Digital e Processo Eletrônico* [Em linha], São Paulo, Saraiva Educação, 2020, pp. 109-111, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786555591484/>, consult. 27.11.2021.

nhecida como Grande Depressão, que foi sentida pelo menos até a Segunda Guerra Mundial, passando pelo fim do Acordo de Bretton Woods com a emergência das moedas fiduciárias e ausência de lastro financeiro[19], até se chegar ao grande impacto sofrido mundialmente pela bolha imobiliária americana de 2008, conhecida como crise dos *subprime*[20], com a emissão desenfreada de moeda por parte dos bancos centrais e a desconfiança nas próprias instituições e em suas políticas econômicas empreendidas.

Por outro lado, este período de surgimento do *bitcoin* pode ser visualizado dentro da chamada Quarta Revolução Industrial, que aprofunda os sistemas digitais e as tecnologias já existentes, trazendo para análise conceitos novos, como desmaterialização, desmonetização, descentralização, distribuição e digitalização[21], com vistas a se entender a evolução do desenvolvimento atual dentro do contexto da intitulada Web3, evolução da até então presente Web2 e que toma como base uma sociedade econômico-digital sem a necessidade de intermediários, baseada em tecnologia criptográfica.

Assim, o *bitcoin* surge como uma verdadeira alternativa às moedas fiduciárias, centralizadas na figura estatal e que tem como base central de existência o conceito de confiança, profundamente abalado diante da grave crise ocasionada em 2008, mesmo período de criação do referido sistema monetário eletrônico desintermediado.

Conforme se verifica do seu documento de fundação, indica-se a inauguração de uma versão direta (*peer-to-peer* ou P2P) para dinheiro eletrônico[22] que permitiria a realização de pagamentos *on-line*, sem a utilização de um intermediário, que neste caso se configuraria como uma instituição financeira. Tal solução se daria, grosso modo, pela utilização de assinaturas digitais através dessa rede desintermediada, com o fim de evitar a ocorrência do chamado gasto duplo, ou seja, que o pagamento com o mesmo valor seja

[19] De julho de 1944 até 15 de agosto de 1971 fora estabelecido o Sistema Bretton Woods de gerenciamento econômico internacional, com a manutenção, por parte dos Estados, de taxa de câmbio com variação de valor indexado ao dólar, o qual, por sua vez, encontrava-se com valor ligado ao ouro em uma base fixa, ou seja, havia o lastro monetário em ouro. Todavia, no governo americano de Richard Nixon, tal conversibilidade entre dólar e ouro foi cancelada, ocasionando o colapso do sistema e a composição da moeda como fiduciária, efetivamente sem lastro e com câmbio flutuante.

[20] Segue-se a indicação de Maria do Carmo Garcez Ghirardi, *Op. Cit*., p. 32, com a assertiva sugestão, para maiores esclarecimentos em relação à crise dos *subprime*, do documentário *Inside Job*, tratando sobre surgimento, crescimento e emergência da intitulada bolha financeira.

[21] Dayana de Carvalho Uhdre, *Blockchain, tokens e criptomoedas: análise jurídica*, São Paulo, Almedina, 2021, p. 18.

[22] Em que pese seja referido no documento originário do *bitcoin* a emergência de dinheiro eletrônico, conforme se verá adiante, verifica-se que a criptomoeda em exame, assim como os demais criptoativos de mesma natureza, configura-se como um tipo de moeda virtual (e não moeda eletrônica), pois não possui lastro em moeda fiduciária de curso forçado nem curso legal, mas possui unidade de medida própria, ao passo que é descentralizada e baseada em tecnologias de criptografia.

feito mais de uma vez, esta justamente a função de segurança exercida pela instituição financeira.

A inovação desse sistema está justamente em eliminar o intermediário que valida e garante a segurança das transações, que ocasionaria o aumento de gastos na realização das transações, mas que seria necessário para evitar (ou ao menos atenuar) a ocorrência de fraudes. Utiliza-se da tecnologia que comumente se intitulou *blockchain*[23], tomando por base um *hash* em cadeias contínuas de prova-de-trabalho (ou *proof-of-work*), formando registros que se objetiva serem inalteráveis (a não ser que seja refeita a prova).

Explica-se também que a confiabilidade do sistema se baseia na circunstância de a maioria dos dispositivos eletrônicos envolvidos serem controlados por participantes cooperantes, ou seja, que não têm intenção de atacar a rede, os quais, de maneira descentralizada e colaborativa, gerarão cadeias mais longas para superar os ditos atacantes.

Portanto, demonstra-se desde já que a confiança em que se baseiam os meios de pagamento, e sobremaneira o comércio eletrônico, que é o foco de criação do *bitcoin*, é substituída por um sistema baseado em prova criptográfica, possibilitando que duas partes, mesmo que desconhecidas e que não nutram qualquer relacionamento de confiança uma com a outra, possam transacionar diretamente sem a necessidade de um terceiro confiável, tendo em vista que estas transações seriam computacionalmente impraticáveis de reverter, protegendo, assim, tanto vendedores como compradores da ocorrência de fraudes.

As transações realizadas com *bitcoin* são definidas pelo próprio artigo como uma cadeia de assinaturas digitais, que vão sendo conferidas através de blocos de informações encadeados e em ordem cronológica através da prova-de-trabalho. Esta função é incentivada através da entrega de moeda para a propriedade de quem efetuar tal comprovação na rede, efetivamente como se ocorresse um garimpo por ouro, pelo que se denominou de atividade de mineração. Registre-se ainda que o incentivo poderá ocorrer através de taxas de transação, pois que não existe autoridade central para emissão dessa moeda.

Afora as condições técnicas de desenvolvimento da rede ainda constantes no documento de criação do *bitcoin*, merece ainda serem destacados dois pontos: a privacidade dos usuários e os cálculos probabilísticos relacionados à possibilidade de empreender fraude ao sistema recém-criado.

Tendo em vista ser descentralizado e público, sendo necessário o anúncio de todas as transações a serem validadas publicamente, tentou-se evidenciar a semelhança desse sistema ao nível de informação divulgada pelas bolsas de valores, em que, em que pese haver divulgação dos negócios individuais em si, a identidade dos participantes é restrita, o que pode ser feito através de pseudônimos ou códigos de identificação.

---

[23] Mais adiante será analisado, ainda que de forma sintética, o modo revolucionário e pioneiro como se desenvolve a concretização dessa tecnologia.

Por outro lado, para empreender a confiabilidade necessária ao sistema, propôs-se já de partida a probabilidade de um atacante se propor a burlar o sistema, na tentativa de gerar uma cadeia alternativa a que foi construída honestamente. Chegou-se à conclusão de que tal probabilidade não poderia ser considerada, tendo em vista a multiplicidade de participantes na rede a trabalharem honestamente, a rapidez com que os blocos vão sendo formados e a necessidade de validação da prova-de-trabalho pela maioria dos que compõem o sistema, tornando, assim, mais dispendioso perpetrar uma fraude, considerando os custos com eletricidade, do que efetivamente o ganho de minerar a própria criptomoeda[24].

Muito embora, em um primeiro momento, a perspectiva desse sistema tenha convencido apenas parte da população com ideal libertário do poderio soberano e tradicional dos Estados nacionais, verificou-se durante os últimos anos crescente utilização do *bitcoin*, principalmente como reserva de valor, sobremaneira no período de crise econômica ocasionada pela disseminação da Covid-19, responsável pela diminuição drástica de cotação de diversas moedas fiduciárias, com ênfase nos países subdesenvolvidos como o Brasil. Saliente-se, por fim, a emergência de diversos outros criptoativos e novas tecnologias lastreadas no mesmo ideal, o que gerou interesse de diversas instituições e organismos internacionais, bem como dos próprios Estados, como adiante se verificará.

2.3. BLOCKCHAIN COMO SUSTENTÁCULO DO SISTEMA

O *bitcoin*, assim, surge como uma *moeda*[25] digital e virtual em alternativa às moedas fiduciárias emitidas pelos Estados, tendo como objetivo, no seu âmago e nas palavras do seu idealizador, ser uma versão puramente *peer-*

---

[24] Para informações mais detalhadas sobre a origem do *bitcoin* a que se alude neste momento, v. Dayana de Carvalho Uhdre, *Op. Cit*., pp. 17-28, e Maria do Carmo Garcez Ghirardi, *Op. Cit*., pp. 17-27.

[25] Utiliza-se o termo destacado por ser entendimento corrente que as criptomoedas não detêm todas as características para serem constituídas juridicamente como moeda, ou seja, servir como meio de pagamento, unidade de conta e reserva de valor, diante da alta volatilidade e da não aplicabilidade maciça pela população. Registre-se, todavia, a doutrina de José Engrácia Antunes (2021a), *As Criptomoedas* [Em linha], 2021, p. 11, disponível em <URL:https://portal.oa.pt/media/133308/jose-engracia-antunes.pdf>, consult. 12.07.2022, que entende se tratar economicamente de tipo monetário emergente, espécie monetária de 4ª geração, após a emergência da moeda física, da bancária e da eletrônica, ainda que admita que o desempenho das tradicionais funções monetárias referidas seja feita de forma parcial, imperfeita e limitada (p. 5). Para maiores detalhes, v. José Engrácia Antunes (2021b), *A Moeda – Estatuto Jurídico e Econômico*, Coimbra, Almedina, 2021, pp. 177-260. Também interessante ver posicionamento, embora minoritário, de Paulo Duarte, "Obrigações de Dinheiro (Obrigações monetárias) e Obrigações de Bitcoins. Estudos de Direito do Consumidor" [Em linha], n° 14, 2018, pp. 343-381, disponível em <http://www.rdmf.es/wp-content/uploads/2018/09/Paulo-Duarte-art%C3%ADculo.pdf>, consult. 30.03.2023, acerca da comparabilidade entre obrigações monetárias e obrigações com *bitcoins*.

-to-peer (ou P2P) de dinheiro eletrônico, permitindo que pagamentos *on-line* fossem enviados diretamente de uma parte para outra, sem passar por uma instituição financeira, em um contexto histórico de desmaterialização, descentralização e digitalização.

Tal só foi possível diante da utilização da tecnologia *blockchain*, um tipo de estrutura de dados distribuída[26], idealizada através da compilação dos dados em blocos de informações encadeados. Assim, com objetivo libertário dos seus usuários, podendo o *bitcoin* ser considerado como moeda deflacionária[27] e proporcionando reserva de valor, a tecnologia que a concretiza pode ser caracterizada como privada, automatizada, auditável, sem órgão regulador ou fiscalizatório, com pretensão de imutabilidade, transparência e desnecessidade de intermediários, obtida pela descentralização da rede e do consenso para validação[28].

Não sendo objetivo deste estudo a comprovação do grau de confiabilidade, tendo em vista que tal já foi ostensivamente comprovado, sendo utilizada largamente por variados atores em ambientes diversos, considera-se que o potencial disruptivo, pioneiro e inovador da *blockchain* possa ser equiparado à revolução trazida pela emergência da Internet, tendo em vista que não se limita às criptomoedas ou mesmo aos próprios criptoativos, possuindo múltiplas utilidades ao se partir como ponto central da ideia de armazenamento e transação de dados tomando por base um sistema dotado de confiança, descentralizado e perene.

Exatamente por isto que a difusão da sua utilização tem como objetivo primário o potencial de ganhos de produtividade nas diversas áreas de implementação, em que se podem destacar, além dos criptoativos de onde surgiu, os ambientes de saúde, energia, suprimento, gerenciamento de propriedade intelectual, de bens móveis e imóveis, expedição de documentos como diplomas de graduação, setor público e até mesmo o mercado financeiro, proporcionando igualmente segurança, transparência e velocidade nas suas atividades.

Trata-se, assim, de um livro caixa diário, público, permanente e de código aberto, com anotação das transações ocorridas na plataforma e o consequente registro para consultas futuras por qualquer interessado. Podem, dessa forma, serem verificadas as inserções de dados feitos pelos demais usuários sem qualquer intermediário, de forma transparente, direta e sem autoridade central. Por outro lado, os blocos são feitos de forma perene e de modo irreversível, pois vinculados às transações anteriormente validadas,

---

26 Ou *Distributed Ledger Technology* (DLT). Todavia, sendo uma espécie do gênero DLT, acabou seu termo sendo disseminado e utilizado de tal forma como se fosse a própria tecnologia de dados distribuída.

27 Fernando Ulrich, *Bitcoin: a moeda na era digital*, São Paulo, Instituto Ludwig von Mises Brasil, 2014, p. 6.

28 Para maior desenvolvimento acerca da caracterização da tecnologia, v. Dayana de Carvalho Uhdre, *Op. Cit*., pp. 29-48.

em um encadeamento lógico, cronológico e sistemático, verificável por todos os participantes.

Tecnicamente e de forma sintética, cada conexão (usuário, nó ou ponto) do *blockchain* detém comunicação direta com todos os outros, sendo identificada por endereço alfanumérico específico de 30 (trinta) caracteres, forma de identificação pretensamente privada que igualmente se aplica às carteiras (ou *wallets*) e contas de usuário, o que, ao mesmo tempo em que torna o ambiente público, limita o acesso de informações das identidades dos utilizadores[29].

Conforme Uhdre[30], a ligação entre os blocos se dá pelos chamados *hash*, verdadeiras impressões digitais de cada bloco, iniciado com a cópia do *hash* do bloco anterior, que, conectando-se ambos os blocos, formará um *hash* unívoco seu, e que simultaneamente iniciará o bloco seguinte. Para tanto, substituindo as instituições financeiras (no caso das criptomoedas) como entes garantidores, criaram-se mecanismos de consenso entre os nós da rede para inserção de novos dados nesse grande livro razão contábil, em que a maioria concorda com a legitimidade dos novos dados de transação para inserção, validando a operação e premiando quem resolveu o problema matemático (no caso do *bitcoin*, com a referida moeda, incluindo as taxas cobradas por todas as transações do bloco minerado, chamadas de *mining fees*).

Assim, além de diversas outras aplicações, graças a tal tecnologia surgem os *smart contracts*[31], que nada mais são do que documentos ou transações inalteráveis depois de realizados, sendo possível, assim, firmar contratos e autorizar transações de acordo com os termos tecnicamente pré-estabelecidos para efetivação do negócio previsto. Com isso, por exemplo, podem ser criados sistemas que agilizem pagamentos internacionais, eliminando intermediários e acontecendo em tempo real, diminuindo custos sem perder de vista a segurança, pois são verificáveis e auditáveis por meio de contratos inteligentes. Da mesma forma, pode ser desenvolvido para desburocratizar a logística da exportação e importação de mercadorias, bem como

---

29 Tendo em vista os fins específicos e limitados deste trabalho, para maiores informações sobre o tema, v. Tiana Laurence, *Blockchain Para Leigos* [Em linha], Rio de Janeiro, Alta Books, 2019, pp. 25-52, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9788550808024/>, consult. 27.11.2021, Bruno Diniz, *O Fenomeno Fintech: tudo sobre o movimento que está transformando o mercado financeiro no Brasil e no mundo* [Em linha], Rio de Janeiro, Alta Books, 2020, pp. 199-205, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9788550815459/>, consult. 27.11.2021, e Susanne Chishti; J. Barberis, *A Revolução Fintech: o manual das startups financeiras* [Em linha], Rio de Janeiro, Alta Books, 2017, pp. 217-221, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786555206760/>, consult. 27.11.2021.

30 Dayana de Carvalho Uhdre, *Op. Cit*., p. 34.

31 Conforme se verifica em Dayana de Carvalho Uhdre, *Op. Cit*., p.50, no contexto da *blockchain*, podem ser entendidos como "códigos, programas computacionais, autoexecutáveis, que, por serem 'processados' em uma infraestrutura descentralizada (blockchain), trazem maior resiliência a mudanças".

firmar um aluguel de imóvel através da integração de contrato inteligente do *blockchain* a uma fechadura inteligente.

Conforme se vê, as possibilidades de utilização e aplicabilidade da tecnologia *blockchain* são quase infinitas, verificando-se, por conseguinte, que o seu desenvolvimento se torna inclusive de pretensa maior importância do que os próprios criptoativos, pois, como se verifica, diversos setores de desenvolvimento de atividades, inclusive não econômicas, têm se utilizado do ideal de sistema para otimizar os seus trabalhos, assim como se deu com o surgimento da rede mundial de computadores.

2.4. PANDEMIA E EMERGÊNCIA DE OUTROS CRIPTOATIVOS

Primeiramente, há que se esclarecer que a *blockchain* é apenas uma espécie de tecnologia baseada em sistema de contabilidade distribuída (DLT), mas que, tendo em vista ter se tornado corrente e mais comum do que o próprio gênero, nem sempre as características são as mesmas das que ocorrem com o *bitcoin* ou outras criptomoedas, como o *ethereum*.

Assim, utilizando-se da classificação dos tipos de *blockchain* empreendida pela Organização para Cooperação e Desenvolvimento Econômico (OCDE) em 2018, constante em Uhdre[32], há dois principais critérios para catalogar os seus tipos, podendo a *blockchain* ser pública ou privada, dependendo da disponibilidade de acesso ao público da plataforma, e ainda ser permissionada ou não permissionada, a depender do nível de permissões exigidas para adição de informações. Nas públicas, portanto, as informações estão abertas para qualquer interessado ler e visualizar, enquanto que as não permissionadas admitem a qualquer um que contribua com a rede, seja por validação ou por adição. Tudo vai depender dos fins destinados com a utilização da tecnologia, o que já denota a multiplicidade de aplicações.

Inclusive, há mesmo a possibilidade de oposição ao conceito inicial libertário com que foi gerado, o que acontece principalmente (mas não somente) com redes privadas e permissionadas, que perdem ao menos parte dos ideais de transparência, desintermediação, imutabilidade e correção de dados. Todavia, não tendo os mesmos fundamentos do *bitcoin*, mas apenas tendo alicerçado a sua viabilidade, tal flexibilidade de estruturas pode ser útil para resolução de problemas e para suprir necessidades relacionadas a negócios específicos, em que por vezes podem ser enfrentadas situações em que seja essencial a mitigação de tais premissas, com a centralização de leitura e verificação de informações (privadas) e/ou limitação de inserção e validação de dados na rede (permissionadas).

Tendo em vista tal diversidade de fenômenos vinculados ao surgimento e desenvolvimento da *blockchain*, a doutrina tem trazido classificação cronológi-

32 Dayana de Carvalho Uhdre, *Op. Cit*., pp. 44-45.

ca baseada em quatro gerações, encontrando-se sintetizada em Uhdre[33], ainda que para fins didáticos, tendo em vista a construção com velocidade exponencial que o fenômeno vem atingindo. Assim, a primeira geração (*Blockchain 1.0*) estaria relacionada à própria origem do *bitcoin*, considerada como sinônimo de criptomoedas, manejada de forma mais simples e, ao mesmo tempo, detendo problemas de eficiência em termos de esforço computacional.

A segunda geração (*Blockchain 2.0*) se liga ao lançamento da plataforma *ethereum*, proporcionando como ideia central servir de plataforma de infraestrutura para outros projetos e aplicabilidades, chamados de *dapps* (*decentralized applications* ou aplicações descentralizadas), ganhando destaque os *smart contracts*, definidos como autoexecutáveis e que usam propriedades de *blockchain*, como resistência à violação, processamento descentralizado e outros[34]. Também neste momento se verifica a existência maciça das chamadas ICO's (*Inicial Coin Offering* ou oferta inicial de moeda), que levou muitos investidores a terem prejuízos consideráveis através de pirâmides financeiras[35].

Por sua vez, a terceira geração (*Blockchain 3.0*), evolução da anterior, privilegiou a utilização da tecnologia nos diversos outros setores além das criptomoedas, destacando-se neste momento o vislumbre de utilidades em atividades governamentais, em contraposição ao discurso inicial de disrupção pela tecnologia, a exemplo das chamadas *Central Bank Digital Currencies* (CBDC's ou Moedas Digitais dos Bancos Centrais). Também é nessa fase que novas funcionalidades são visualizadas, como a interoperabilidade entre plataformas e aumento de velocidade da rede, com vistas à sua escalabilidade. É neste momento em que também se verifica o surgimento das finanças descentralizadas (DeFi), com o objetivo de promover atividades, serviços e produtos eminentemente bancários e/ou financeiros sem a intermediação de uma instituição garantidora.

Por fim, a atual quarta geração (*Blockchain 4.0*) tem como norte a utilização da inteligência artificial com base nos recentes desenvolvimentos, emergindo o conceito de *blockchain* como serviço (BaaS) e melhora nas condições de eficiência de consenso e de consumo de energia, com soluções mais amigáveis e perceptíveis ao consumo de massa, ampliando o seu nicho de aplicação com o fim de popularização e difusão de utilizadores. É neste momento que se verifica a necessidade de evolução das interfaces para usuários, com vistas a atingir maior público-alvo, bem como se almeja, por exemplo, amenizar o sensível problema de consumo de energia ocasionado pela corrida desenfreada pela mineração de criptoativos como o *bitcoin*, atra-

---

33 Dayana de Carvalho Uhdre, *Op. Cit*., p. 55.

34 Eublockchain, "European Union Comission. Legal and Regulatory Framework of Blockchain and Smart Contracts" [Em linha], Setembro de 2019, disponível em <URL:https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf>, consult. 27.11.2021.

35 Este foi um dos grandes e graves problemas verificados pelas autoridades estatais e financeiras quando do surgimento das criptomoedas, conforme se verá nos próximos capítulos.

vés da tentativa de utilização de energia limpa, produzida a partir de fontes renováveis, ou mesmo a emergência de *tokens* de crédito de carbono.

Verifica-se, desse modo, que a evolução da tecnologia *blockchain* foi acompanhada necessariamente pela diversificação dos tipos de serviços relacionados, em que importa para este estudo a evolução dos criptoativos existentes na economia. Para tanto, desde já se informa que, utilizando classificação trazida pela *International Organization for Standardization* (ISO 22739:2020), considera-se criptoativo como qualquer ativo digital implementado usando tecnologia criptográfica, caracterizado como espécie de gênero intitulado *token*[36], que diferencia a existência do bem na realidade digital (criptoativo nativo de *blockchain*) ou ainda os ativos ditos *tokenizados*, ou seja, representações eletrônicas e criptografadas de ativos do mundo real[37]. Todavia, entende-se que a circunstância de ser um criptoativo ou um ativo *tokenizado* não tem o condão de diferenciar o enquadramento jurídico a ser dado ao bem digital, mas aparentemente apenas procura facilitar o entendimento diferencial da origem do respectivo ativo.

Por sua vez, verificando-se a análise minuciosa empreendida por Uhdre[38] no que concerne à catalogação das diversas classificações dos tipos de *tokens*, concorda-se com a necessidade de se centrar, para a devida classificação jurídica do fenômeno, na função exercida por cada ativo, ao passo que se utiliza a mais usual divisão tripartite, sobremaneira no formato descrito pela OCDE[39], diante da importância internacional de tal organização[40]. Entende-se, assim, pela existência dos *payment tokens* (basicamente as criptomoedas), que, destinados ao exercício de funções monetárias, podem se destinar tanto a meio de troca ou de pagamento, a ser reserva de valor e/ou a unidade de medida; *security tokens*, relacionados de uma forma geral

---

36 Segundo Dayana de Carvalho Uhdre, *Op. Cit*., p. 61, entenda-se *token* como "representações digitais e criptografadas de ativos. E essas representações podem se referir tanto a ativos existente no mundo 'real', físico — daí se falar em 'tokenização de ativos' (verdadeiros 'avatares' desses bens ou direitos) — quanto a ativos nativos e exclusivos do mundo virtual (nativos de blockchain), caso em que estaríamos diante dos 'criptoativos' em sentido estrito, digamos assim."

37 Assim, concordando com o entendimento de Dayana de Carvalho Uhdre, *Op. Cit*., p. 89, que faz justamente tal diferenciação, *token* é gênero que tem como espécies os criptoativos e os ativos tokenizados.

38 Dayana de Carvalho Uhdre, *Op. Cit*., pp. 57-97.

39 OECD, "OECD Blockchain Primer" [Em linha], 2018, disponível em <URL:https://www.oecd.org/finance/ OECD-Blockchain-Primer.pdf>, consult. 27.11.2021.

40 Ainda que, como já se disse, esta classificação não preencha todas as realidades apresentadas, porém se utiliza por ser usualmente conhecida e aplicada.

aos valores mobiliários[41]; e *utility tokens*, classificação residual que representa grosso modo um direito a um bem ou serviço[42].

Esta classificação também se encontra em consonância com guia publicado pelo Tribunal de Contas da União brasileiro[43], que cataloga os *tokens* em pagamento, utilitários e ativos, estes representativos de valores mobiliários. A importância do esclarecimento de catalogação por parte da doutrina é relevante para constituir subsídio ao plano legislativo, designadamente no que respeita à natureza jurídica e regulação do respectivo mercado, bem como a tributação dessas manifestações de riqueza.

Tal função, nesse ponto concordante com Uhdre[44], deve ser verificada a partir do *whitepaper* explicativo do criptoativo para se concluir pela funcionalidade dentro do sistema, o que, obviamente, não deve ser estanque, mas flexível à medida que a tecnologia relacionada evolua e possa abranger outras realidades, inclusive de se configurar como híbrido, pelo que há de se considerar, nesses casos, a função predominantemente exercida, bem como possibilitar a constante alteração de natureza jurídica ou classificação.

Desse modo, além de se verificar a complexidade e quantidade diferente de classificações e catalogações dos tipos de *tokens*, o que, mesmo se utilizando da tripartição de funções, pode gerar diferenças de entendimento, há que se evidenciar que o mercado de criptoativos está em constante evolução, principalmente durante a pandemia em que se escreve este trabalho, cenário de desenvolvimento de possibilidades infinitas.

Não se tem como intuito, tendo em vista os objetivos específicos deste estudo, o aprofundamento na caracterização e diferenciação dos diversos criptoativos atualmente existentes, tendo em vista inclusive que, diante da efervescência da utilização de tais tecnologias, as funcionalidades vão sendo desenvolvidas em tempo real, o que prejudica até mesmo o objetivo de sistematização e simplificação do entendimento do leitor, ao passo que a doutrina igualmente não nutre tempo necessário para promover cientificamente tal intento.

Todavia, com vistas a constatar que a regulação estatal não se encontra em consonância com a realidade do mundo real (incluindo o cenário virtual em exame), de forma ainda mais atrasada e vacilante na criptoeconomia, fenômeno muito novo e que necessita de profundo conhecimento espe-

41 Relacionados às figuras tradicionais no mercado de ações e bolsas de valores, a exemplo de ações, debêntures, bônus de subscrição, opções, swaps, mercado a termo e mercado de futuros.

42 Sendo residual, para viabilização do projeto a que se destina, pode se ligar a apenas um ou mais propósitos pelo adquirente, como destinar direito a voto, proporcionar funcionalidades em plataformas ou até preferência na aquisição de produtos ou serviços.

43 Tribunal de Contas da União, "Levantamento da tecnologia blockchain" [Em linha], 2020, p. 17, disponível em <URL:https://portal.tcu.gov.br/data/files/59/02/40/6E/C4854710A7AE4547E18818A8/ Blockchain_sumario_executivo.pdf>, consult. 27.11.2021.

44 Dayana de Carvalho Uhdre, *Op. Cit*., p. 87.

cializado, importa registrar o surgimento dos NFT's (*tokens* não fungíveis), enquanto possibilidade de financiamento e desenvolvimento econômico em ramos como da cultura (arte e música), esportes (*fan tokens*) e games; dos STO's (*Secutity Token Offering*) enquanto contrato de investimento em um ativo subjacente[45]; dos ETF's (*Exchange Traded Funds*) de criptoativos, enquanto fundos de investimento negociados na bolsa de valores e que funcionam de forma similar aos outros produtos do mercado; bem como do universo de DeFi (finanças descentralizadas), verdadeiramente um mundo a parte neste universo e que promete revolucionar o ambiente bancário e financeiro. Por fim, destaque-se ainda a realidade da tokenização de ativos, que, segundo recentes pesquisas, tem o potencial de movimentar cifras trilionárias nos próximos anos[46].

2.5. ABRANGÊNCIA DO MERCADO, INVESTIMENTOS INSTITUCIONAIS E *STABLECOINS*

Para o que importa ao presente trabalho, desde a criação do *bitcoin*, a própria tecnologia *blockchain* vem evoluindo de forma considerável. Iniciando-se como suporte para o registro das transações com criptomoedas, a criação da plataforma *ethereum* verdadeiramente transformou o ambiente dos criptoativos, pois possibilitou a existência dos *smart contracts*, bem como a ampliação da gama de possibilidades de utilização. Os avanços tecnológicos possibilitaram maior interoperabilidade, escalabilidade e diferenciação de consensos, com maior eficiência e economia de energia, tornando-se mais popular a utilização de novas aplicações, a exemplo dos *tokens* não fungíveis no mercado de arte e jogos, fundos de investimento no mercado de valores mobiliários, finanças descentralizadas no mercado financeiro e até mesmo a viabilidade da chamada *Central Bank Digital Currency* (CBDC) enquanto formato digital da moeda fiduciária com curso legal em determinado Estado[47].

Diante do mercado trilionário dos criptoativos[48], considerando a atual crise ocasionada pela disseminação da Covid-19, acostumamo-nos com

---

45 O que o diferencia das ICO's, que, em sua maioria, posicionam sua moeda como *utility token* e que dá aos usuários acesso à plataforma nativa ou aplicativos descentralizados (DApps), bem como das IPO's (*Initial Public Offering*), ligadas ao mercado tradicional enquanto ações de uma empresa vendidas ao público em geral numa bolsa de valores, através da abertura do capital.

46 Notícias de dois desses relatórios disponíveis em <URL:https://exame.com/future-of-money/opiniao-entenda-a-tokenizacao-de-ativos-novo-mercado-de-us-16-trilhoes-ate-2030/> e <URL:https://cointelegraph.com.br/news/tokenization-of-illiquid-assets-to-reach-16t-by-2030-report>, consult. 15.04.2023.

47 Igualmente, para esclarecimentos sobre os termos utilizados, v. Dayana de Carvalho Uhdre, *Op. Cit*., pp. 49-55.

48 O valor do *Market Cap* pode ser verificado em: <URL:https://coinmarketcap.com/charts/>, consult. 27.11.2021. Também há que se salientar o considerável e vertiginoso aumento de valor das diversas espécies de criptoativos. No caso do *bitcoin*, até meados de 2009 nem mesmo tinha um valor estipulado, já que sua primeira cotação aconteceria somente alguns meses depois, em 05 de outubro, quando a *New Liberty Standard* avaliou

notícias acerca do investimento de consolidadas instituições no mercado cripto como um ativo alternativo de reserva de valor, a exemplo da fabricante de veículos Tesla, do banco de investimentos JP Morgan, da líder mundial no fornecimento de plataformas analíticas e software de mobilidade MicroStrategy e das empresas de pagamentos *on-line* Paypal e Square, bem como sobre declarações positivas de figuras públicas como Elon Musk, Michael J. Saylor e Ray Dalio.

Diante do aumento expressivo tanto do número de investidores como do volume total do mercado, impulsionado pela multiplicidade de aplicações além das já conhecidas criptomoedas, como os NFT's, verdadeira revolução no mercado artístico e esportivo, e ainda as atividades de finanças descentralizadas a oferecerem diversos produtos e possibilidades de cunho financeiro e bancário, os organismos e instituições internacionais e os próprios Estados nacionais estão procurando se especializar no assunto, com vistas a compreender melhor o fenômeno para regulá-lo e igualmente se valer dele para benefícios próprios.

Nesse contexto surgem as *stablecoins*[49], que são criptomoedas atreladas a algum tipo de ativo, adquirindo, portanto, certa estabilidade nos valores de suas unidades. Em sua tipologia com lastro em moeda fiduciária, por exemplo, possibilita a emissão de *tokens* que sejam representativos da respectiva moeda em circulação escolhida. Foi exatamente o projeto Libra (agora Diem), capitaneado pelo então Facebook (atual Meta), que causou bastante polêmica e preocupação sobre a sua eventual aceitação generalizada pela população como meio de pagamento. Ocorreram audições no Congresso Americano e no Parlamento Europeu, face ao risco do Facebook lançar este criptoativo com potencial de uso pelos mais de um bilhão de usuários das suas redes sociais como forma de pagamento de bens e serviços, o que poderia ocasionar prejuízos à estabilidade econômica diante da capilaridade real e concreta da empresa e o poderio econômico do grupo.

Assim, neste contexto histórico são inseridas as CBDC's (*Central Bank Digital Currencies*), que já seriam evolução do objetivo anterior, através da emissão da moeda oficial de um Estado já em ambiente inteiramente virtual, tornando o próprio *token* como moeda oficial do ente. Está-se em análise

que 1 (um) dólar poderia comprar pouco mais de 1300 (mil e trezentas) unidades (1300 BTC's equivalem a mais ou menos 80 milhões de dólares na cotação em que se elabora o trabalho). Por sua vez, começando-se a operar a moeda digital em 06 de janeiro de 2010, a DWDollar avaliou sua cotação em 0,001 dólar. Por fim, em sua primeira transação comercial, pagou-se 10000 (dez mil) BTC's por uma pizza de 25 (vinte e cinco) dólares, o que equivaleria a aproximadamente 600 milhões de dólares na cotação histórica atingida em dezembro de 2021.

49 Novamente pela definição de Dayana de Carvalho Uhdre (2021, p. 92), estas "surgiram como resposta à volatilidade das criptomoedas. Ao se atrelar as unidades de criptomoedas a ativos (ou cesto de ativos), lastreando-as, portanto, em 'algo de valor', a tendência seria a de se manter certa estabilidade nos valores daquelas unidades. Nessa lógica, seria possível aos Estados emitirem tokens representativos de suas moedas-fiat em circulação".

tal implementação em vários países pelo mundo, com destaque da China com o yuan digital, bem como projeto avançado do Real digital no Brasil e discussões avançadas sobre a possibilidade de implantação do Euro digital em solo europeu.

Por isso, há necessidade de se diferenciar, neste momento, as definições de moeda digital, moeda virtual, moeda eletrônica e criptomoedas, diferente do entendimento de Ghirardi[50] que especifica se tratarem de sinônimos. Para tanto, inicialmente se entende como moeda digital o gênero de ativo que proporciona a circulação de valor por meio eletrônico ou via Internet, em que se subdivide nas demais espécies. Por sua vez, utiliza-se o pensamento de Teixeira[51], através de diferenciação do que entende o Banco Central do Brasil por moeda eletrônica, aquela moeda real inserida em um sistema eletrônico, conforme disposto na Lei 12.865/2013, e por moedas virtuais, que não são emitidas por nenhum governo soberano, possuindo forma própria de dominação, não representando dispositivo ou sistema eletrônico para armazenamento em reais (ou qualquer outra moeda fiduciária), não sendo, assim, autorizada nos termos do art. 18 da referida legislação nacional brasileira, pois que o emitente não é considerado instituição financeira e, como consequência, a circulação da moeda não é entendida como atividade bancária para fins legais e regulatórios.

Por fim, em que pese tanto a moeda virtual como a criptomoeda possuírem características em comum, nomeadamente não possuir lastro em moeda fiduciária, possuir unidade de medida própria, não possuir curso legal nem curso forçado[52], a virtual se diferencia por ser centralizada e não se basear necessariamente em tecnologias de criptografia, como, por exemplo, os programas de fidelidade para acúmulo de milhas aéreas[53].

---

50 Maria do Carmo Garcez Ghirardi, *Op. Cit*., p. 24.

51 Tarcísio Teixeira, *Op. Cit*., p. 110.

52 Conforme se verifica em José Engrácia Antunes (2021a), *Op. Cit*., p. 17, as criptomoedas possuem curso convencional, portanto, não sendo de aceitação obrigatória e poder liberatório, dependem de acordo das partes na transação envolvida. Para maiores detalhes, v. José Engrácia Antunes (2021b), *Op. Cit*., pp. 217-220.

53 Em José Engrácia Antunes (2021a), *Op. Cit*., p. 5, em classificação um pouco diferente, insere o conceito de moedas virtuais como gênero (assim como fora colocado o conceito de moeda digital), do qual são espécies as moedas de valor intrínseco (como as libras de ouro), as moedas locais (como as notas "pago em lixo" portuguesas), e as moedas digitais de uso restrito (como moedas utilizadas em jogos eletrônicos, milhas aéreas ou para fidelização de clientes). Por sua vez, trata as criptomoedas (embora depois trazendo este conceito para as demais espécies de criptoativos) como moedas virtuais em sentido estrito, ao passo que retira as moedas bancárias e eletrônicas do escopo das moedas virtuais, pois estas não tem entidade emitente, assentam em sistema descentralizado ou desintermediado de circulação, estão denominadas em unidade de conta própria, não são livremente convertíveis em outras espécies monetárias e não possuem quadro legal de regulação e supervisão próprio.

Concluindo, verifica-se a clara e expressiva importância monetária e financeira do mercado de criptoativos, o que faz com que a sua regulação, em um ambiente inteiramente virtual, seja de suma importância aos Estados nacionais. Diante dos problemas identificados e enfrentados, da atualidade e ausência de harmonização de entendimento sobre o fenômeno, e das diferenças de tratamento regulatório em cada país, vislumbra-se a necessidade de se analisar o contexto de maneira globalizada, em superação ao entendimento tradicional de soberania, temáticas que serão enfrentadas nos próximos capítulos.

3. PROBLEMAS IDENTIFICADOS NO COMÉRCIO DE CRIPTOATIVOS

Muito embora, nos primeiros anos de existência do *bitcoin*, as instituições e organismos nacionais e internacionais não tenham dado a devida atenção ao fenômeno, com a natural evolução e múltiplas alternativas de utilização da tecnologia *blockchain* no desenvolvimento de negócios econômicos e financeiros não regulados, foram identificadas problemáticas à medida que a procura e envolvimento foi aumentando. A multiplicidade e diversificação de criptoativos, baseados em tecnologia, descentralização, criptografia e algoritmos, igualmente potencializa a capilaridade dos serviços prestados, sobremaneira diante da pandemia ocasionada pela disseminação da Covid-19, que propiciou a emergência da digitalização em todos os âmbitos da vida em sociedade.

Sem o intuito de esgotar o tema e com vistas a didaticamente proporcionar entendimento assertivo, elencam-se cinco riscos relevantes observados pelos Estados e organismos internacionais para regulação do setor, quais sejam, cometimento de ilícitos, tributação do mercado, proteção dos investidores, higidez do sistema financeiro e monetário, e sustentabilidade socioambiental. Assim, enquadrada a importância e atualidade da criptoeconomia no capítulo anterior, utiliza-se deste momento para delimitar os pontos mais sensíveis a serem discutidos nas esferas governamentais para proporcionar segurança jurídica e equilíbrio neste âmbito.

3.1. FACILIDADE PARA COMETIMENTO DE ILÍCITOS

A utilização de criptoativos para cometimento de ilícitos é um fenômeno presente desde os primeiros anos de existência do *bitcoin*, iniciando-se as investigações e notícias de crimes cometidos na mesma proporção da sua popularização, ao passo que, em que pese as discussões doutrinárias se concentrarem na utilização de criptomoedas como objeto material, os mesmos raciocínios aqui trazidos são igualmente válidos para o conjunto da criptoeconomia, a exemplo dos NFT's, do universo de DeFi e ainda do cres-

cente interesse no embrionário mercado do metaverso[54], todos passíveis de serem utilizados como instrumentos de práticas criminosas.

Inicialmente ligada à discussão acerca da ilegalidade das criptomoedas e a tipicidade do delito de moeda falsa, o que já foi superado diante do entendimento majoritário de que não se tratam juridicamente de moeda[55], figuram-se os crimes piramidais como segunda geração de preocupações em matéria penal, que, por questões didáticas, será tratada em discussão própria acerca da proteção dos investidores.

Por sua vez, já tratando da terceira geração desta escala de preocupações, verifica-se a existência do intitulado trilema penal econômico[56], em que são englobadas as figuras distintas dos crimes de evasão de divisas[57], sonegação fiscal[58] e lavagem de dinheiro (ou branqueamento de capitais), em que este último delito, seguramente, detém visão superlativa nesta equação, sobremaneira por proporcionar o financiamento ao tráfico ilícito de entorpecentes e ao terrorismo, bem como outros delitos antecedentes caracterizados dentro da criminalidade organizada transnacional que atualmente se observa.

---

54 Antes utilizado apenas em obras de ficção científica, muitas empresas estão investindo neste tipo de tecnologia, que basicamente alia a internet, a realidade aumentada e a realidade física aprimorada para produzir um espaço virtual compartilhado. Com múltiplas possibilidades de aplicação prática, gigantes como Facebook, Google, Microsoft, Samsung e Sony se uniram em consórcio para modelar o futuro dessa realidade dita experimental. Disponível em <URL:https://exame.com/future-of-money/metaverso-o-que-e-a-relacao-com-cripto-e-como-isso-vai-mudar-a-sua-vida/>, consult. 23.12.2021. Os desenvolvimentos já encontram como norte a existência de multiverso, ou seja, a interligação de metaversos.

55 Conforme Thiago Rufalco Medaglia e Eric Simões Visini, "Breves considerações sobre o tratamento legal, contábil e fiscal das moedas virtuais", *In Tributação da economia digital: desafios no Brasil, experiência internacional e novas perspectivas* [Em linha], Monteiro, Alexandre Luiz Moraes do Rêgo; Faria, Renato Vilela; Silveira, Ricardo Maitto da,. São Paulo, Saraiva, 2018, pp. 625-641, disponível em <URLS:https://integrada.minhabiblioteca.com.br/#/books/9788553604500/>, consult. 02.01.2022, p. 628, "a prática internacional demonstra que a maioria dos países ainda restringe o conceito de moedas àquelas emitidas, reguladas ou admitidas pelas respectivas legislações internas. A experiência internacional sugere que a maioria dos países não atribui o caráter de 'moeda' às moedas virtuais, embora exceções sejam encontradas".

56 Utiliza-se esta classificação em gerações e igualmente a referência ao trilema penal econômico feita por Renato de Mello Jorge Silveira, "Criptocrime": considerações penais econômicas sobre criptomoedas e criptoativos", *in Rev. de Direito Penal Econômico e Compliance* [Em linha], Vol. 1, 2020, disponível em <URL:https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/white-paper/rdpec-1-renato-de-mello.pdf>, consult. 23.12.2022, pp. 2-5.

57 Também por questões didáticas, será tratado este delito no Capítulo III, tendo em vista se tratar especificamente da legislação penal brasileira.

58 Pelo mesmo motivo supracitado, problemática a ser enfrentada a seguir, em conjunto com o tema da tributação das riquezas na criptoeconomia.

Há que se entender que a presente discussão se encontra inserida nos chamados crimes de informática[59] ou cibercriminalidade[60], que, de modo geral, vem aumentando vertiginosamente nos últimos anos[61]. Neste sentido, a utilização de criptomoedas (principalmente o *bitcoin*) como meio de pagamento a crimes de sequestro, roubo e *ramsomware*[62] se tornou frequente, diante da pretensa condição de anonimato da identidade dos beneficiários. Dumbra[63] faz relação direta da migração de alguns crimes para o meio digital diante da ocorrência de abundância de informações, muitas disponibilizadas voluntariamente, e da possibilidade de se ocultar a identidade de conexão, a hospedagem do *website* utilizado em servidores internacionais e a facilidade de propagação do vírus[64] utilizado em várias partes do mundo simultaneamente, o que, em contrapartida, dificulta as autoridades de investigação em identificar a origem do ataque e a responsabilização dos envolvidos.

Tendo em vista a limitação deste trabalho e o objetivo a que se destina[65], diante da multiplicidade de conceitos entre diversos doutrinadores, docu-

---

59 Utiliza-se tal terminologia advinda de Tarcísio Teixeira, *Op. Cit*., p. 214, que define crime de informática como aquele praticado utilizando meios informáticos como instrumento de alcance ao resultado pretendido ou aquele praticado contra os sistemas e meios informáticos. Este é o aspecto penal inserido no gênero Direito da Informática, enquanto estudo do Direito sobre os problemas jurídicos que ocorrem no uso da Tecnologia da Informação. Por sua vez, o mesmo autor ainda classifica os crimes de informática entre próprios, relacionados aos ataques contra os sistemas de informática, e os impróprios, que utilizam a informática como instrumento para sua execução, ou seja, aqueles delitos já existentes e que podem ser cometidos pela internet.

60 Nomenclatura reconhecida pela legislação portuguesa, como transposição da ordem jurídica europeia.

61 Conforme se verifica do Relatório Cibersegurança em Portugal Riscos & Conflitos 2021, do Centro Nacional de Cibersegurança Portugal, constatou-se aumento significativo no volume de incidentes de cibersegurança e nos números dos indicadores de cibercrime em 2020. Disponível em <URL:https://www.cncs.gov.pt/docs/relatorio-riscosconflitos-2021-observatoriociberseguranca-cncs.pdf>, consult. 23.12.2021.

62 Conforme Bruno de Morais Dumbra, "Sequestro de dados e terrorismo digital: os atuais tipos penais são suficientes para punir os crimes em ambiente virtual?", *In Direito e Novas Tecnologias* [Em linha], São Paulo, Almedina Brasil, 2020, pp. 73-88, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 23.12.2021, p. 75, é o sequestro de dados, em que o criminoso chantageia a vítima através da indisponibilização de seus dados com criptografia, fornecendo a chave para desbloqueio apenas mediante o pagamento de resgate, que frequentemente é feito sob moeda virtual.

63 Bruno de Morais Dumbra, *Op. Cit*., p. 79.

64 Mesmo ciente da existência de diversos tipos de ataques a computadores, entenda-se o termo *vírus* como gênero, unicamente para facilitar a compreensão do fenômeno.

65 Para maiores detalhes sobre a temática relacionada à lavagem de dinheiro de uma forma geral, indica-se a doutrina de Luiz Regis Prado, *Direito Penal Econômico* [Em linha], 9ª ed., Rio de Janeiro, Forense, 2021, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786559641192/>, consult. 23.12.2021 e André Luís Callegari, *Lavagem de Dinheiro* [Em linha], 2ª ed. rev., atual. e ampl., São Paulo, Atlas, 2017, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9788597012293/>, consult. 23.12.2021, bem como o trabalho de Maria Balbina Martins de Rizzo, *Prevenção da lavagem de dinheiro nas organi-*

mentos[66] e organismos internacionais[67], além dos órgãos nacionais de investigação e inteligência[68], porém sempre convergindo em seus aspectos comuns, utiliza-se do conceito de Braga[69] para se considerar lavagem de dinheiro como "*todo o processo mediante o qual se oculta ou dissimula a existência, a fonte ilegal, a procedência, o movimento e o destino de bens procedentes de atividades ilegais, com o fim de criar uma aparência lícita*".

Destaque-se, nesta seara, o Grupo de Ação Financeira Internacional (GAFI, ou *Financial Action Task Force* - FATF), criado pelo G7 em 1989 em Paris, França, por membros da OCDE, enquanto organização de vanguarda no combate à lavagem de dinheiro e ao financiamento do terrorismo em escala global. Nesta seara surgem suas paradigmáticas 40 Recomendações[70]

---

zações [Em linha], 2ª ed. atual. e rev., São Paulo, Trevisan, 2016, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9788599519875/>, consult. 23.12.2021, especificamente no âmbito da prevenção da lavagem de dinheiro nas organizações.

66 Dentro do chamado sistema internacional antilavagem de dinheiro, destacam-se a Declaração de Princípios de Basileia intitulado "Prevenção do uso ilícito do sistema bancário para atividades de lavagem de dinheiro", aprovado em 12.12.1988, pelo Comitê sobre Regulamentação e Práticas de Controle das Operações Bancárias; a Convenção das Nações Unidas contra o Tráfico Ilícito de Entupefacientes e Substâncias Psicotrópicas (chamada de Convenção de Viena de 1988), aprovada pela Assembleia Geral das Nações Unidas, de 25.11.1988 a 20.12.1988; a Convenção Relativa ao Branqueamento, Detecção, Apreensão e Perda dos Produtos do Crime (chamada de Convenção de Estrasburgo, de 1990), depois substituída pela Convenção do Conselho da Europa Relativa ao Branqueamento, Detecção, Apreensão e Perda dos Produtos do Crime e ao Financiamento do Terrorismo, de 16.05.2005; a Convenção Interamericana contra a Corrupção, celebrada em Caracas, Venezuela, em 1996; A Convenção Internacional para a Supressão do Financiamento do Terrorismo, celebrada em Nova York, EUA, em 1999; a Convenção das Nações Unidas Contra a Criminalidade Organizada Transnacional (chamada de Convenção de Palermo, de 2000); a Convenção Interamericana contra o Terrorismo, celebrada em Bridgetown, Barbados, em 2002; e a Convenção das Nações Unidas contra a Corrupção, celebrada em Mérida, México, em 2003.

67 Com destaque para o Grupo de Egmont, que reúne 159 unidades de inteligência financeira (UIF's) como plataforma de intercâmbio seguro de informações financeiras para combater a lavagem de dinheiro e o financiamento ao terrorismo; o Conselho de Segurança, a Comissão das Nações Unidas para Lavagem de Dinheiro (*Law Enforcement, Organized Crime and Anti-Money-Laundering Unit*) e o próprio Escritório das Nações Unidas sobre Drogas e Crimes (*United Nations Office on Drugs and Crime* - UNODC); a Organização para Cooperação e Desenvolvimento Econômico (OCDE); a Interpol (Organização Internacional de Polícia Criminal) e a Europol (serviço europeu de polícia).

68 No Brasil, o Conselho de Controle de Atividades Financeiras (COAF), que é a Unidade de Inteligência Financeira (UIF), e, para o desenvolvimento de planos de ação conjuntos, a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA) e o Programa Nacional de Combate à Lavagem de Dinheiro (PNCLD). Em Portugal, a Unidade de Informação Financeira ligada à Polícia Judiciária. Nos Estados Unidos da América, a *Financial Crimes Enforcement Network* (FinCEN) enquanto UIF nacional.

69 Romulo Rhemo Palitot Braga, *Lavagem de dinheiro: fenomenologia, bem jurídico protegido e aspectos penais relevantes*, 2ª ed., Curitiba, Juruá, 2013, p. 126.

70 Na sequência dos atentados terroristas de 11 de setembro de 2001, foram elaboradas mais 9 recomendações para combate ao financiamento do terrorismo. Por fim, pas-

com o fim de aperfeiçoar os sistemas jurídicos nacionais na luta contra o fenômeno, reforçando o impulso da cooperação internacional e estabelecendo didaticamente as três fases ou etapas do delito que foram reproduzidos nas legislações estatais: colocação ou ocultação (*placement*)[71], conversão ou transformação (*layering*)[72], e integração/reintegração (*integration*)[73] dos bens no sistema legal.

Verifica-se quanto ao delito lavagem de dinheiro que há evidente e clara ligação com a utilização da *deep web* e da *dark web*,[74] que se baseiam na ideia de anonimização[75] para comercialização de toda sorte de itens e produtos no mercado negro, como drogas, armas, pornografia infantil e dados obtidos de forma ilegal, utilizando-se principalmente de *bitcoins*[76] como método de pagamento[77].

Elucidativa e bastante atual a comparação feita por Mendroni[78] em relação às técnicas de lavagem de capitais com o surgimento de uma vacina para o

sando por nova revisão em fevereiro de 2012, foram novamente condensadas em 40 recomendações para abranger o combate à utilização do sistema financeiro para proliferação de armas de destruição de massa. Conforme se verá, documento igualmente atualizado no contexto da criptoeconomia.

71 Distribuição do "dinheiro sujo", em efetivo ou espécie, no sistema financeiro ou na economia do país.

72 Pretensão de dotar de aparência lícita, mediante fraude, o objeto lavado, dificultando o rastreamento dos recursos provenientes das atividades ilícitas e tentando tirar o caráter *sujo* do dinheiro.

73 Inserção do ativo no sistema econômico e financeiro, sendo a fase de legitimação dos recursos.

74 Navega-se na internet na chamada *surface*, com indexação e acesso aos sítios eletrônicos pelos motores de busca. Enquanto na *deep web* não há indexação do conteúdo pelos mecanismos de busca, acessível por *softwares* específicos que usam redes criptografadas para ocultar a identidade do usuário, na *dark web* se permite o compartilhamento de dados de maneira pretensamente anônima e criptografada, com tecnologia mais complexa para utilização, que pode exigir até alteração de *hardware* para acesso (Renato de Mello Jorge Silveira, *Op. Cit*., pp. 2-3).

75 Existem *softwares* como *The Onion Router* (Tor)*, Invisible Internet Project* (i2p) *e o Freenet,* que permitem a navegação em certas partes inacessíveis aos *browsers* comuns, em que se esconde o IP dos utilizadores e dos servidores, os quais permitem a navegação anônima.

76 Emblemático o caso *Silk Road*, espécie de mercado negro na Internet onde eram comercializadas mercadorias ilícitas mediante o pagamento em *bitcoins*, em que se chegou ao montante de 158 milhões de dólares confiscados (Renato de Mello Jorge Silveira, *Bitcoin e suas fronteiras penais: em busca do marco penal das criptomoedas*, Belo Horizonte, D' Plácido, 2018, p. 113).

77 Manuel Fletes, diretor do Instituto dos Profissionais de Prevenção à Lavagem de Dinheiro, afirma que em 2019 cerca de 829 milhões de dólares foram transacionados pela *dark web*, sugerindo que as plataformas de criptomoedas deveriam ser mais zelosas. Disponível em <URL: https://veja.abril.com.br/economia/carteis-de-drogas-usam-bitcoins-para-lavar-dinheiro/>, consult. 23.12.2021.

78 Marcelo Bartlouni Mendroni, *Crime de lavagem de dinheiro* [Em linha], 4ª ed. rev., atual. e ampl., São Paulo, Atlas, 2018, p. 207, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9788597016796/>, consult. 23.12.2021.

combate a uma doença, em que apenas após causar consideráveis danos à população que os cientistas conseguem entender o seu mecanismo para poder desenvolver uma cura para contê-la, igualmente ocorrendo o mesmo com a saúde financeira dos governos e da população com o referido crime. Assim, conclui que a utilização de criptomoedas como modalidade de lavagem de dinheiro já é realidade entre grupos terroristas como o Estado Islâmico, tendo em vista a deficiência na identificação dos usuários, inexistência de órgão central responsável pelo fornecimento de informações às autoridades de investigação, liquidez nas operações, inclusive com utilização de cartões de crédito e débito, e a existência de criptografia nas operações[79].

Muito embora ciente da existência de entendimento doutrinário acerca da impossibilidade de utilização de criptoativos como objeto material ao cometimento do delito de lavagem de dinheiro[80], perfilha-se à doutrina majoritária que entende tal ser plenamente possível, tendo em vista que, conforme Florêncio Filho e Castanheira[81], no ambiente virtual se torna viável qualquer das fases da lavagem, seja colocação, ocultação e integração, ficando tudo muito fluido e passível de ser viabilizado.

Assim, utilizando-se da conclusão de Telles[82] acerca dos *bitcoins* como objeto material do delito de lavagem de dinheiro, tendo em vista a sua natureza de bem incorpóreo, chega-se igualmente a esta possibilidade em relação ao conjunto dos criptoativos, por estarem inseridos no conceito genérico de bem como objeto de direito e adquirindo valor de troca no mercado[83]. Na mesma obra demonstra como obstáculos apresentados na criptoeconomia podem ser contornados diante da apresentação de ambiente especialmente favorável ao cometimento de ilícitos, que proporciona anonimato, facilidade de manuseio, possibilidade de manipular preços e de operar em diferentes jurisdições simultaneamente sem existência de uma autoridade central[84].

---

79 Ibidem, p. 262.

80 A título de exemplo, Tiana Laurence, *Op. Cit*., p. 197.

81 Marco Aurélio Florêncio Filho e Yasmin Abrão Pancini Castanheira, "Prevenção à Lavagem de Dinheio em Cryptocurrencies Exchanges" *In Direito Penal Econômico* [Em linha], Cury, Rogério, São Paulo, Almedina, 2020, pp. 105-130, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556270531/>, consult. 23.12.2021, p. 115.

82 Christiana Mariani da Silva Telles, *Sistema Bitcoin, Lavagem de Dinheiro e Regulação*, Dissertação (Mestrado em Direito), Escola de Direito da Fundação Getúlio Vargas, Rio de Janeiro, 2018, p. 66.

83 Conforme Pierpaolo Cruz Bottini; Gustavo Henrique Badaró, *Lavagem de dinheiro: aspectos penais e processuais penais: comentários à Lei 9.613/1998, com as alterações da Lei 12.683/2012*, São Paulo, Revista dos Tribunais, 2016, p. 110, seriam coisas que carregam alguma espécie de valor.

84 "Com efeito, conforme mencionado acima, existem tecnologias de anonimização que são capazes de tornar os bitcoins inteiramente anônimos ou, ao menos, dificultar sobremaneira seu rastreamento. A alta volatilidade dos preços dos bitcoins, também como demonstrado, pode igualmente servir como fator para incentivar o uso da criptomoeda em questão, já que pode ser bastante proveitosa para criminosos interessados em gerar ganhos artificiais de forma aparentemente lícita. O fato de o mercado de bitcoins ainda ser

Também se verifica em Estellita[85], analisando tese de doutorado de Johanna Grzywotz, que conclui que o uso de moedas virtuais incrementa o risco de lavagem de dinheiro, considerando as características de descentralização[86], pseudoanonimidade[87] e globalidade[88], com ausência de controle rigoroso e de trocas de informações das instituições financeiras e de crédito, que têm como base e norte de atuação tendência mundial de extinção dos sigilos bancário e fiscal. Assim, principalmente em países com medidas de controle antilavagem menos rigorosas, pode-se facilmente proceder à integração dos valores adquiridos por origem ilícita, seja através de trocas por moedas estatais em *exchanges* ou se utilizando dos contratos inteligentes intitulados *swaps* atômicos[89], aquisição direta de bens e produtos, investimento em uma ICO ou até mesmo simples apresentação como resultado de um empreendimento lucrativo ou de valorização do ativo.

reduzido, por sua vez, pode facilitar a manipulação de preços, permitindo seu aumento ou diminuição artificial" (Christiana Mariani da Silva Telles, *Op. Cit*., p. 81).

85 Heloisa Estellita, "Criptomoedas e lavagem de dinheiro", *in Rev. Direito FGV* [Em linha], n° 1, Vol. 16, 2020, pp. 3-5, disponível em <URL:https://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/issue/view/4501/2488>, consult. 24.12.2021.

86 Além de negociações através de *exchanges*, existem plataformas que proporcionam transações diretas e até em espécie, além de caixas eletrônicos, venda de bens ilícitos com remuneração em criptomoedas, cartões de crédito e débito para criptoativos, que proporcionam a fase de colocação. A prática de *smurfing* ou estruturação (fracionamento de grande quantia em pequenos valores, de forma a escapar dos órgãos de controle) também é plenamente exequível.

87 Além de existirem jurisdições que ainda não exigem ferramentas de *Know Your Client* (KYC) para usuários do setor, em que há ausência de identificação clara e concreta para abertura de contas, podem ser criados endereços e chaves para cada transação, o que dificulta o rastreamento. Há ainda possibilidades mais complexas para a concretização da conversão, como a utilização de métodos para mascarar a publicidade característica da *blockchain*, chamados de *tumblers* ou *mixers*, que são serviços terceirizados que objetivam interromper a conexão entre emissores e receptores mediante o pagamento de taxa para verdadeiras misturas entre os bens de outros usuários, o que, por outro lado, igualmente pode proporcionar riscos de furtos, desvios ou perda destes valores. Desde que com o fim de simples anonimização para privacidade, o serviço é considerado legal. Saliente-se, por fim, a existência de criptomoedas que se alega serem totalmente anônimas, como o Monero (XMR), o NAVcoin (NAV), o ShadowCash (SDC) e o Darkcoin (DRK), as quais fogem do escopo deste estudo.

88 Alguns fatores a serem considerados são: velocidade da transação, facilidade de transporte dos valores com manuseio por chaves digitais criptografadas, dificuldade de rastreamento com dependência de peritos e técnicos especializados, dificuldade de localização pelos juízes e polícia para concretização de penhoras e confiscos, e dificuldade de definir as leis de regência e dos tribunais competentes para o deslinde de tais investigações e julgamentos.

89 Formato de troca de criptoativos entre duas *blockhains* diferentes ou até fora da comunidade *blockchain*, podendo ser feita de carteira para carteira sem envolver trocas a terceiros.

Desta forma, diante de revisão doutrinária e de dados atualizados sobre o setor[90], inclusive com indicações de empresas especializadas no assunto[91], utiliza-se da conclusão feita por Andrade[92] em momento anterior à realidade atual para, em revisão do seu entendimento, afirmar que, ante a incompletude ou deficiência de regulação e a especialização de práticas criminosas que usam o ciberespaço como ambiente, pode-se associar a expansão do fluxo criminoso ao uso de criptoativos, sobremaneira através de criptomoedas.

3.2. DIFICULDADES DE TRIBUTAÇÃO DAS MANIFESTAÇÕES DE RIQUEZAS

Tendo em vista se tratar de cifras bilionárias que diariamente são comercializadas no mercado de criptoativos[93], torna-se questão basilar entre os Estados a definição de critérios para incidência fiscal e tributária, tomando-se tanto a natureza jurídica dos bens em si envolvidos como igualmente a clarificação sobre o fato gerador a incidir na respectiva matriz do tributo a ser recolhido aos cofres públicos. A visão de Castagna[94] resume de forma objetiva as dificuldades enfrentadas nesta seara.

---

90 Em relatório de 2017, a Europol já trazia análise acerca da utilização da *darknet* para tráfico de drogas. Disponível em <URL:https://europol.europa.eu/cms/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf>, consult. 24.12.2021. Em relatório de 2018, a empresa Cipher Trace já apontava crescimento de delitos com criptomoedas, com estimativa de 1,3 bilhões de dólares lavados em ferramentas como *tumblers*. Disponível em <URL:https://cryptographybuzz.com/cryptocurrency-laundered-bitcoin/>, consult. 24.12.2021. A Polícia Federal do Brasil apreendeu 130 milhões de reais em criptomoedas usadas em lavagem de dinheiro no ano de 2020, o que equivale a metade do total apreendido nesse tipo de delito. Disponível em <URL:https://www.gov.br/pt-br/noticias/justica-e-seguranca/2020/12/combate-a-corrupcao-e-ao-trafico-de-drogas-estiveram-na-mira-do-governo-em-2020>, consult. 24.12.2021.

91 A empresa Chainalysis, em audiência pública da Comissão da Câmara dos Deputados para revisão da Lei nº 9.613/1998, a lei antilavagem brasileira, sugeriu que os criptoativos sejam expressamente incluídos na nova lei a ser implementada no país. Disponível em <URL:https://exame.com/future-of-money/criptoativos/chainalysis-sugere-incluir-cripto-em-lei-de-lavagem-de-dinheiro-no-brasil/>, consult. 24.12.2021.

92 Mariana Dionísio de Andrade, "Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro", *in Rev. Bras. de Políticas Públicas* [Em linha], n° 3, Vol. 7, 2017, p. 57, disponível em <URL:https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4897/3645>, consult. 24.12.2021.

93 Conforme se verifica do sítio eletrônico disponível em <URL:https://coinmarketcap.com/charts/>, consult. 31.12.2021.

94 "O exercício das competências tributárias enfrenta, diuturnamente, desafios das mais variadas ordens, no contexto de um processo de legitimação que varia entre a função distributiva da tributação, a justificação constitucional das imposições tributárias, os paradigmas do direito natural ou normativo de propriedade, até os obstáculos de ordem pragmática, sobretudo na adequada normatização das regras-matrizes de incidência, à luz dos limites e garantias do contribuinte, e a eficiente identificação dos eventos sociais que, vertidos em linguagem, constituem-se em fatos jurídico-tributários, ingressando no universo jurídico" (Ricardo Alessandro Castagna, "Blockchain e operações financeiras: impactos na tributação", *In Direito e Novas Tecnologias* [Em linha], Costa-Corrêa, André;

Utilizando-se das observações quanto à realidade do delito de lavagem de dinheiro, as mesmas dificuldades são encontradas na seara tributário-fiscal, pois que a utilização da *blockchain* proporciona dificuldades quanto à fiscalização, controle e rastreabilidade de eventos sociais eleitos na norma tributária geral e abstrata, considerando o cenário de descentralização e desintermediação. Assim, diante desta evolução tecnológica disruptiva, exige-se exame minucioso para revisão dos tradicionais paradigmas legislativos e regulatórios de eficiência, com possibilidade de adoção de novas estruturas de obrigações acessórias e poderes fiscalizatórios. Possibilita-se, desse modo, impactar o sistema como um todo com vistas à identificação do negócio jurídico em si considerado para fins de lançamento, seja de ofício[95] ou por homologação[96], bem como dos sujeitos passivos relacionados ao evento que relevam para fins de capacidade contributiva, igualdade tributária[97] e isonomia[98], em respeito ao princípio da livre concorrência[99].

Predolim, Emerson Alvarez; Longhi, Maria Isabel Carvalho Sica; Rebouças, Rodrigo Fernandes, São Paulo, Almedina Brasil, 2020, pp. 555-590, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 02.01.2022, p. 555).

95 Momento em que se exigirá da autoridade tributária que identifique todos os signos tributários de forma antecipada.

96 Diante do contexto em que inserida a criptoeconomia, entende-se que a tributação se dá fundamentalmente por homologação, o que igualmente exige que a autoridade tributária tenha conhecimento do setor para poder fiscalizar e convalidar os negócios jurídico-tributários informados pelos contribuintes.

97 Para Sacha Calmon Navarro Coêlho, *Curso de Direito Tributário Brasileiro* [Em linha], 17ª ed., Rio de Janeiro, Forense, 2020, p. 51, disponível em <URL:https://integrada.minhabiblioteca.com.br/#/books/9788530988357/>, consult. 02.01.2022, a "capacidade contributiva é o motor operacional do princípio da igualdade na esfera tributária, tendo o condão, por isso mesmo, de realizar o próprio valor justiça", ou seja, igualdade em condições iguais de capacidade contributiva.

98 Conforme Kiyoshi Harada, *Direito financeiro e tributário* [Em linha], 30ª ed., São Paulo, Atlas, 2021, disponível em <URL:https://integrada.minhabiblioteca.com.br/#/books/9786559770038/>, consult. 02.01.2022, p. 447, por princípio tributário se "veda o tratamento jurídico diferenciado de pessoas sob os mesmos pressupostos de fato; impede discriminações tributárias, privilegiando ou favorecendo determinadas pessoas físicas ou jurídicas". Registre-se que essa compreensão é aplicável tanto no sentido de tributar como no sentido inverso de isentar ou beneficiar.

99 Ricardo Alessandro Castagna, *Op. Cit*., pp. 571-582. Conforme em Luis Eduardo Schoueri, *Direito Tributário* [Em linha], São Paulo, Saraiva Educação, 2021, p. 210 disponível em <URL:https://integrada.minhabiblioteca.com.br/#/books/9786555592696/>, consult. 02.01.2022, "o princípio da livre concorrência atua igualmente como limite para a atuação do legislador tributário: cabe a este investigar os efeitos danosos que pode gerar sobre a concorrência, mitigando-os". Assim, há que se entender que com isto se preserva o princípio da neutralidade concorrencial da tributação, para que não se influencie indevidamente na atuação dos *players* no mercado.

Inegável a possibilidade de ocorrência de infrações tributárias[100] no setor econômico dos criptoativos[101], seja por evasão, sonegação ou fraude fiscal[102], ou ainda por comportamentos dentro do contexto de planejamento fiscal abusivo ou agressivo[103]. Além da pseudoanonimização com a utilização de *mixing services*, que dificulta a própria identificação do patrimônio do contribuinte, conforme Telles[104], a alta volatilidade dos valores dos ativos e a possibilidade concreta de manipulação de preços proporcionam campo fértil para produção de cenários artificiais, seja no sentido de ganhos para fins de lavagem de dinheiro como no sentido de perda para fins de ilícitos tributários.

Deste modo, a instituição de mecanismos eficientes de trocas de informações entre as administrações para identificação de ilícitos fiscais, bem como para cobrança e recolhimento adequado de tributos, enseja a necessidade de cooperação entre os Estados no combate à fraude fiscal, com evolução das áreas de fiscalização diante de sistemas informáticos mais padronizados para facilitar a agilidade nas informações a serem trocadas. Tudo com base na exigência de transparência fiscal e combate aos regimes que proporcionam sigilo ou segredo bancário e fiscal de forma desmedida, intitulados paraísos fiscais[105], bem como, por outro lado, apoiado em ins-

---

100 Conforme Glória Teixeira, *Op. Cit*., p. 355, adota-se a criminalidade fiscal como subcategoria da categoria geral intitulada de criminalidade econômica.

101 Como exemplos, podem ser citados os trabalhos de David Montezuma Mota Ribeiro, *Bitcoin e Direito Penal: uma breve análise da moeda virtual como meio para o crime de sonegação fiscal* [Em linha], Instituto Brasileiro de Direito Penal Econômico, 2021, disponível em <URL:https://ibdpe.com.br/bitcoin-e-direito-penal-uma-breve-analise-da-moeda-virtual-como-meio-para-o-crime-de-sonegacao-fiscal/>, consult. 02.01.2022, e Leandro Bastos Nunes, "O Bitcoin-cabo na condição de meio para a consumação de crimes econômicos" [Em linha], Associação Nacional do Ministério Público, disponível em <ULR:https://www.anpr.org.br/imprensa/artigos/25690-o-bitcoin-cabo-na-condicao-de-meio-para-a-consumacao-de-crimes-economicos>, consult. 02.01.2022, acerca da utilização de criptomoedas como meio para o crime de sonegação fiscal, inclusive na modalidade *bitcoin*-cabo, em que o ilícito é cometido sem o bem ser efetivamente enviado ao exterior.

102 Diferenciando sonegação de fraude fiscal, Luiz Regis Prado, *Op. Cit*., p. 409, estabelece que "sonegação é toda ação ou omissão dolosa tendente a impedir ou retardar, total ou parcialmente, o conhecimento por parte da autoridade fazendária: I) da ocorrência do fato gerador da obrigação tributária principal, sua natureza ou circunstâncias materiais; II) das condições pessoais do contribuinte, suscetíveis de afetar a obrigação tributária principal ou o crédito tributário correspondente". Por sua vez, conceitua fraude como "toda ação ou omissão dolosa tendente a impedir ou retardar, total ou parcialmente, a ocorrência do fato gerador da obrigação tributária principal, ou a excluir ou modificar as suas características essenciais, de modo a reduzir o montante do imposto devido, ou a evitar ou diferir o seu pagamento".

103 Conceituação novamente retirada de Glória Teixeira, *Op. Cit*., p. 360, com fins de simplificação e diferenciação com a ilicitude tributária. Assim, muito embora considerados lícitos, tais atos têm como consequência a aplicação de medidas antiabuso como a correção da matéria coletável.

104 Christiana Mariani da Silva Telles, *Op. Cit*., p. 74.

105 Destaque-se a Convenção sobre Assistência Mútua Administrativa em Matéria Fiscal, de 1988, por parceria entre a OCDE e os Estados-membros do Conselho da Europa,

trumentos inspetivos e mecanismos legais preventivos e repressivos válidos, em consonância com os direitos fundamentais dos cidadãos, nomeadamente o respeito à privacidade, proporcionalidade no acesso aos dados pessoais e à legalidade das condutas empreendidas[106].

Inserido no contexto da economia digital, em sua perspectiva internacional diante da realidade de desmaterialização e desterritorialização, com destaque para o comércio eletrônico ou *e-commerce*[107], há que se destacar que a criptoeconomia é um fenômeno que potencializou a pulverização das relações comerciais, que já se encontravam facilitadas com a chegada da informática e da rede mundial de computadores, tendo em vista que a ausência de limites territoriais e a possibilidade de transmissão de dados e bens de maneira virtual e em tempo real se tornam ainda mais rápida, em ritmo e montante assustadores. O que chama a atenção das autoridades nacionais e também das mais diversas organizações internacionais, que já vêm há décadas se dedicando aos problemas advindos do comércio eletrônico internacional[108]. Todavia, destaque-se que os problemas jurídicos no espaço virtual são potencializados se os países cujas partes envolvidas (fornecedor e consumidor) estejam sediadas não forem signatários de nenhum acordo mútuo ou documento internacional que preveja a relação em análise.

Dessa forma, com a facilidade da comercialização de produtos via Internet, a possibilidade de sonegação fiscal aumenta vertiginosamente, surgindo inúmeros comerciantes informais que realizam suas operações sem o devido recolhimento dos tributos relacionados, contexto em que as plataformas de comércio eletrônico ou *marketplaces* adquirem especial relevância, por serem veículos para muitos usuários comercializarem eficientemente seus produtos. Por isso, procura-se responsabilizar tais interfaces para fins de recolhimento dos tributos indiretos incidentes nas operações por elas inter-

o qual já sofreu protocolo de alteração em 2011. Espera-se que cada vez mais países possam ratificar seus termos, proporcionando ambiente de segurança jurídica, eficiência e padronização de condutas. Disponível em <URL: https://www.oecd.org/ctp/exchange-of-tax-information/POR-Amended-Convention.pdf>, consult. 31.12.2021.

106 Para maiores esclarecimentos, indica-se Glória Teixeira, *Op. Cit*., pp. 350-368.

107 Para os efeitos deste trabalho, utiliza-se do conceito de Tarcísio Teixeira, *Op. Cit*., p. 182, acerca do comércio eletrônico próprio ou direto como o conjunto de operações de compra e venda de mercadorias e prestação de serviços realizados por intermédio de meios digitais, em que todas as etapas se perfazem na Internet.

108 Destaque-se a Comissão das Nações Unidas para o Direito Comercial Internacional (*United Nations Comission for International Trade Law* - UNCITRAL), que elaborou a Lei Modelo em 1996; a Organização Mundial do Comércio (OMC), que idealizou a Declaração de Genebra sobre o Comércio Eletrônico Global, e realizou a Conferência Ministerial de Seattle; a Convenção de Viena de 1980 (Tratado sobre Contratos de Compra e Venda Internacional de Mercadorias, no âmbito da Comissão das Nações Unidas para o Direito Mercantil Internacional), que visa disciplinar as relações entre empresas, e a *Convention on Contracts for the Internacional Sale of Goods* (CISG), que visa regular contratos internacionais de compra e venda.

mediadas em razão da posição privilegiada neste intercâmbio comercial, em homenagem aos princípios de eficiência e eficácia administrativa.

Em resumo, conforme se visualiza em Medaglia e Visini[109], está-se diante de revolução tecnológica que, enquanto proporciona o retorno do escambo ao centro da prática econômica, ainda que de modo virtual, trouxe verdadeiro questionamento de dogma centenário, que privilegiava os Estados como centros e exclusivos reguladores de políticas monetárias, diante da multiplicidade de atores desregulados que se destacam na criptoeconomia[110].

Além disto, ressalte-se que a problemática é ainda mais evidente dentro do contexto de virtualização em que estão inseridos os criptoativos, tendo em vista que até mesmo a natureza jurídica de cada bem transacionado está igualmente sendo discutida, o que impacta decisivamente na constituição do crédito tributário a ser convertido aos cofres públicos dos Estados, pois que, dependendo da ordem regulatória instituída, as consequências arrecadatórias podem ser totalmente diferentes, bem como as obrigações acessórias respectivas que os contribuintes devem cumprir.

Exemplo disto é a discussão acerca da natureza jurídica das criptomoedas. Em que pese a maior parte da literatura estrangeira não considerar o *bitcoin* juridicamente uma moeda, caracterizando-se, em geral, com pequenas variações, como um bem incorpóreo que serve como meio de troca[111], verifica-se em Neves e Cíceri[112] que a tributação das criptomoedas tem sido adotada de acordo com três classificações: ativo sujeito à tributação de ganho de capital[113], moeda estrangeira[114] ou método de pagamento alternativo[115]. Neste último caso, de forma análoga aos meios de pagamento com

---

109 Thiago Rufalco Medaglia e Eric Simões Visini, *Op. Cit*., p. 626.

110 Essencial afirmar, conforme Guilherme Campos Maia, *O Enquadramento Jurídico-Fiscal dos Criptoativos em sede de IRS*, Dissertação (Mestrado em Direito), Universidade Católica Portuguesa, Porto, 2019, p. 15, que embora exista classificação dos criptoativos entre *payment, utility* e *secutiry tokens*, que igualmente se utiliza para este trabalho, além de não ser unanimemente utilizada, as fronteiras entre as categorias não são rígidas, o que proporciona a existência de verdadeiros híbridos enquanto combinações destas, o que potencializa as possíveis diferenças de tratamento nos Estados diante do entendimento de cada autoridade governamental competente, o que se verá nos próximos capítulos.

111 Christiana Mariani da Silva Telles, *Op. Cit*., p. 54.

112 Barbara das Neves e Pedro Vitor Botan CÍCERI, "Tributação dos criptoativos no Brasil: desafios das tecnologias disruptivas e o tratamento tributário brasileiro", *in Rev. Jurídica da Escola Superior de Advocacia da OAB-PR* [Em linha], n° 3, ano 3, 2018, pp. 125-163, disponível em <URLS:http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2018/12/revista_esa_8_07.pdf>, consult. 02.01.2022, p. 142.

113 Conforme se verifica no Brasil, nos Estados Unidos e na Austrália.

114 *Bundesminis-terium der Finanzen* da Alemanha, no dia 01.03.2018, publicou diretiva neste sentido.

115 Conforme decidiu o Tribunal de Justiça da União Europeia em processo envolvendo Administração Fiscal da Suécia e David Hedqvist (Processo C-264/14). Disponível em <URL:https://curia.europa.eu/juris/liste.jsf?num=C-264/14>, consult. 02.01.2022.

valor liberatório, tendo em vista que, pelo princípio da autonomia privada, tal poder liberatório deve ser contratualizado[116].

Está-se aqui a tratar acerca dos princípios basilares da legalidade e tipicidade. Conforme se vislumbra de Carvalho[117], somente através de lei se poderá fazer descrição da regra matriz de incidência tributária, aumentar os tributos já existentes, majorar sua base de cálculo ou alíquota, devendo ser estabelecidos no bojo da norma os elementos descritivos do fato jurídico e dos dados da relação obrigacional. Por sinal, diante do que preveem os artigos 109 e 110 do Código Tributário Nacional brasileiro, conforme Torres[118], deve haver consonância entre os institutos, conceitos e formas de Direito Privado com o que se estatui no Direito Tributário, só sendo cabível fazer qualquer alteração quando não se tratar de tipo constitucionalmente considerado como critério para repartição de competências em matéria tributária.

Como outra expressão da legalidade dos tributos, o princípio da tipicidade tributária é dirigido ao legislador e ao próprio aplicador da lei. Conforme Amaro[119] (2021, p. 56), o legislador deve definir, de modo taxativo e completo, as situações tributáveis cuja ocorrência será necessária e suficiente ao nascimento da obrigação tributária, bem como os critérios de quantificação do tributo, enquanto que ao aplicador da lei é vedada a interpretação extensiva e a analogia, sob pena de incorrer em inconstitucionalidade por afronta direta ao princípio da legalidade[120].

---

116 Para maiores esclarecimentos sobre a discussão acerca da natureza jurídica das criptomoedas, com base no *bitcoin*, indica-se Luana Steffens e Cláudio Tessari, "A tributação das operações com criptomoedas no Brasil: o caso da bitcoin", *in Rev. de Direito Tributário Contemporâneo* [Em linha], Vol. 30, 2021, pp. 269-296, disponível em <URL:http://tessaripohlmann.adv.br/wp-content/uploads/2021/09/artigo-39.pdf>, consult. 02.01.2022, Tathiane Piscitelli, "Criptomoedas e os possíveis encaminhamentos tributários à luz da legislação nacional", *in Rev. Direito Tributário Atual* [Em linha], São Paulo, IBDT, n° 40, 2018, pp. 572-590, disponível em <URL:https://ibdt.org.br/RDTA/wp-content/uploads/2018/11/Tathiane-Piscitelli.pdf>, consult. 02.01.2022, e Liziane Angelotti Meira, Fillipe Soares Dall'ora e Hadassah Laís S. Santana, Meira, Liziane Angelotti; Dall'ora, Fillipe Soares; Santana, Hadassah Laís S., "Tributação de novas tecnologias: o caso das criptomoedas" *In Tributação 4.0* [Em linha], Santana, Hadassah, L.; Afonso, José Roberto, São Paulo, Almedina Brasil, 2020, pp. 341-356, disponível em <URL:https://integrada.minhabiblioteca.com.br/#/books/9788584936274/>, consult. 02.01.2022, destacando-se, da última obra, entendimento de que as ICO's não poderão ser comparadas às ofertas no mercado de ações diante da inexistência de órgãos regulatórios para o setor que garantam estrutura e funcionamento com o mínimo de confiança.

117 Paulo de Barros Carvalho, *Curso de direito tributário*, 10ª ed., São Paulo, Saraiva, 1998, p. 98.

118 Heleno Taveira Torres, *Direito tributário e direito privado*, São Paulo, Revista dos Tribunais, 2003, p. 81.

119 Luciano Amaro, *Direito tributário brasileiro* [Em linha], 24ª ed., São Paulo, Saraiva Educação, 2021, p. 56, disponível em <URL:https://integrada.minhabiblioteca.com.br/#/books/9786555592993/>, consult. 02.01.2022.

120 Tal vedação também se encontra inserida no art. 11, nº 4, da Lei Geral Tributária portuguesa. Sobre o cabimento dos princípios da neutralidade, equidade e não-discriminação, igualmente pertinentes ao presente trabalho, conferir Glória Teixeira, *Op. Cit*., pp. 50-56.

Com isto, trata-se de desafio complexo o respeito ao princípio da capacidade econômica enquanto limite ao legislador tributário e ao poder de tributar do Estado e, ao mesmo tempo, de proteção ao contribuinte, pois que, além da definição da natureza jurídica dos negócios econômicos inseridos na transação de criptoativos, há que se verificar, como consequência, se haverá tributo previsto de acordo com as normas constitucionais e legais existentes no respectivo ordenamento jurídico, em homenagem ao princípio basilar da segurança jurídica, que inadmite interpretações unicamente em favor do aumento da arrecadação[121].

Por fim, há que se notar que as análises doutrinárias também se prestam a analisar conceitos importantes e bastante debatidos no campo fiscal, os quais emergem com profunda importância na economia digital. Como exemplos: conceito de estabelecimento tributário permanente[122] ou estável[123]; revisitação do entendimento da tributação pelo Estado da fonte da renda oriunda do comércio eletrônico na esfera internacional[124]; desafios relacio-

---

121 Tarcísio Teixeira, *Op. Cit*., p. 197.

122 Jonathan Barros Vita, "Serviços virtuais e a localização da prestação do serviço: (re) analisando o conceito de estabelecimento tributário no direito brasileiro e internacional", *In Direito e Novas Tecnologias* [Em linha], Costa-Corrêa, André; Predolim, Emerson Alvarez; Longhi, Maria Isabel Carvalho Sica; Rebouças, Rodrigo Fernandes, São Paulo, Almedina Brasil, 2020, pp. 301 a 314, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 02.01.2022, conceituando estabelecimento permanente como estrutura jurídico-tributária que equivale a um centro de imputação de renda, faz análise comparativa entre o direito brasileiro e internacional, utilizando-se do relatório BEPS da OCDE em suas ações 01, 05 e 07, e a Lei Modelo da UNCITRAL. Entende que, diante da possibilidade de criação de ficções jurídicas ou critérios mais distintos para sua determinação, desde que se permaneça como subclasse do estabelecimento desenhado no direito privado (art. 110, do CTN), estão sendo reavaliados conceitos por conta das novas formas eletrônicas de prestação de serviços.

123 Na Espanha houve alargamento do conceito para o comércio eletrônico, ao considerar que empresa estrangeira que possui sítio eletrônico e servidor localizado no país e que conclua contratos de compra e venda será qualificada como estabelecimento estável.

124 Resumidamente, Luis Eduardo Schoueri, "Tributação da renda oriunda do comércio eletrônico na esfera internacional: de volta à tributação pelo Estado da fonte", *In Direito e Novas Tecnologias* [Em linha], Costa-Corrêa, André; Predolim, Emerson Alvarez; Longhi, Maria Isabel Carvalho Sica; Rebouças, Rodrigo Fernandes, São Paulo, Almedina Brasil, 2020, pp. 375 a 396, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 02.01.2022, ao reconhecer que a realidade virtual oferece a dificuldade de não haver conexão suficiente do agente econômico com qualquer Estado e, como consequência, incidir a dupla não tributação, aponta a tributação pelo Estado da fonte como mais viável para os desafios da economia digital, embora os legisladores nacionais tenham dificuldade em avançar neste ponto. Tomando por base princípios de eficiência, simplicidade, neutralidade, capacidade contributiva, exequibilidade e local de consumo, conclui pioneiramente pela opção de tributação pela fonte de pagamento como meio mais adequado diante da capacidade de fiscalização em um meio eletrônico que se aperfeiçoa por transações instantâneas. Assim, usando o exemplo da computação em nuvem, entende não haver argumentos sólidos para justificar tributação distinta entre residentes e não residentes em um mesmo ambiente virtual cujo acesso não está condicio-

nados à tributação dos jogos eletrônicos[125], que detém ligação direta com os NFT's e movimenta cifras expressivas de riqueza[126]; estrutura e funcionalidades dos contratos digitais, que são ofertados, aceitos e gerenciados inteiramente dentro de ambiente digital[127]; e ainda, dentro do contexto contratual, a proeminência dos *smart contracts* enquanto linguagem computacional de programação de sistemas, não alterável pelas partes envolvidas após sua

nado à localização do contribuinte, concluindo pelo critério do mercado consumidor como diferencial para a separação dos negócios celebrados no ambiente interno ou no exterior.

125 Lucas de Lima Carvalho Pedro Amorim, "A tributação dos jogos eletrônicos no Brasil: perspectivas e desafios", *In Direito e Novas Tecnologias* [Em linha], Costa-Corrêa, André; Predolim, Emerson Alvarez; Longhi, Maria Isabel Carvalho Sica; Rebouças, Rodrigo Fernandes, São Paulo, Almedina Brasil, 2020, pp. 315-358, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 02.01.2022, p. 325, considerando se tratar de espécie do gênero da tributação de *software* no Brasil, entende que "tributar ou não uma determinada operação intrajogo depender[á] da existência de um mercado oficial ou paralelo que a suporte". Distinguindo entre operações ocorridas inteiramente no ambiente virtual e aquelas iniciadas e/ou concluídas em ambiente real, dispõe que a real distinção guarda relação com o princípio da realização da renda e do correspondente signo de capacidade contributiva (p. 342), entendendo, de forma minoritária, que as operações intrajogo devem guardar no mundo real a mesma natureza jurídica que revelam no mundo virtual. Por exemplo, caso seja feita prestação de serviços intrajogo, deve assim ser tributada.

126 Destaque-se, diante da longevidade de existência, da plataforma virtual *Second Life*. Criada em 1999 e lançada em 2003, mantida pela empresa Linden Lab, já fez milionários da vida real e, inclusive, já proporcionou disputas judiciais. Disponível em <URL:https://www.conjur.com.br/2009-ago-25/disputas-second-life-chegam-justica-vida-real>, consult. 02.01.2022.

127 Diante da classificação de Natália Kuchar, "Contratos digitais: status atual e novas fronteiras", *In Direito e Novas Tecnologias* [Em linha], Costa-Corrêa, André; Predolim, Emerson Alvarez; Longhi, Maria Isabel Carvalho Sica; Rebouças, Rodrigo Fernandes, São Paulo, Almedina Brasil, 2020, pp. 481-502, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 02.01.2022, p. 483, diferenciam-se dos contratos eletrônicos ou telemáticos, a exemplo de transação de bens materiais em meio virtual. Discorrendo sobre os problemas relacionados ao início da produção de efeitos e às formas de provas destes contratos, destaca a popularização dos *smart contracts*, idealizados pelo jurista e cientista da computação Nick Szabo em artigo intitulado *Smart Contracts: Building Blocks for Digital Markets*, com base nos objetivos de *observability, verifiability, privity* e *enforceability,* e que tem como ponto de destaque a emergência da plataforma *Ethereum* (*Secure Decentralised Generalised Tran-saction Ledger*), que possui linguagem de programação específica chamada Solidity. Disponível em <URL:https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html>, consult. 02.01.2022.

definição inicial[128], largamente utilizado em diversos segmentos econômicos, inclusive fora da utilização inicial em criptoativos[129].

Demonstra-se, desse modo, a abrangência, importância e polêmica que o tema vem sendo enfrentado pelos órgãos e organismos governamentais nacionais e internacionais, com sobreposição de competências que exige cooperação, respeito, trocas de experiências e de informações entre todos os envolvidos.

3.3. NECESSÁRIA PROTEÇÃO DE INVESTIDORES NO DESENVOLVIMENTO DOS SERVIÇOS

Ao mesmo tempo, vislumbra-se certa ausência de garantias, segurança jurídica e econômica para os investidores nas relações existentes no mercado, não sendo raros casos de ataques cibernéticos que resultaram em prejuízos milionários, como ocorreu com a Binance[130], maior plataforma de compra e venda de criptomoedas no mundo, e mais recentemente com a Criptomoeda Pancake Bunny[131], nativo da plataforma de mesmo nome de DeFi.

Outra motivação para o necessário aprimoramento do aparelho legislativo de cada Estado ocorre em decorrência da captação pública de valores, como já ocorre, por exemplo, através de fundos de investimento com as ofertas de *token* que representa valores mobiliários ou STO's (*Security Token Offering*). Trata-se de uma integração das ações tradicionais de bolsas de valores com a tecnologia *blockchain*, que une os conceitos de uma ICO (podem ser usados para garantir o direito a um serviço ou produto oferecido pela Organização Descentralizada ou Aplicativo Descentralizado que a lançou) e uma IPO (mecanismo de Ofertas Públicas de ações de uma empresa que está entrando no mercado financeiro pela primeira vez), o que significa

---

128 Rodrigo Fernandes Rebouças, *Contratos Eletrônicos***,** 2ª ed., Almedina, São Paulo, 2018, pp. 143-147, destaca que os *smarts contracts* não são nova modalidade de contrato, mas tão somente uma nova forma de contratação, em seu formato misto. Também os caracteriza como contratos eletrônicos autoexecutáveis e intersistêmicos em sua fase de eficácia contratual, sendo sua maior preocupação a garantia da execução e adimplemento, ou seja, gerar segurança jurídica aos envolvidos (Rodrigo Fernandes Rebouças, "Contratos eletrônicos: smart contracts"**,** *In Direito e Novas Tecnologias* [Em linha], Costa-Corrêa, André; Predolim, Emerson Alvarez; Longhi, Maria Isabel Carvalho Sica; Rebouças, Rodrigo Fernandes, São Paulo, Almedina Brasil, 2020, pp. 591 a 616, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 02.01.2022, p. 596).

129 Tatiana Revoredo, *Blockchain: tudo o que você precisa saber*, 1ª ed., Amazon, The Global Strategy, 2019, pp. 223-241.

130 Disponível em <URL:https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2019/05/09/corretora-de-bitcoin-binance-sofre-ataque-hacker-que-desvia-us-41-milhoes.ghtml>, consult. 10.06.2020.

131 Conforme: <URL:https://tecnoblog.net/444254/hacker-causa-prejuizo-de-us-200-milhoes-com-roubo-de-criptomoedas/>, consult. 10.06.2020.

que o detentor de uma STO possui um *token* que representa, por exemplo, ações, títulos de dívida, fundos ou fundos de investimento imobiliário[132].

Assim, pela ausência de regulamentação especialmente pensada para este mercado, que padece da intensa volatilidade de preço de seus ativos e de assimetria de informações entre os seus usuários, existe exposição a fraudes e atividades ilícitas[133], a exemplo dos crimes piramidais[134]; a riscos operacionais, como furtos de bens e informações pessoais via *cyber hacking*; a reduzida liquidez, diante da possível ausência de vendedores ou compradores no cenário almejado; e ainda a possibilidade de perda de parte ou totalidade do investimento ao se aventurar em projetos de empresas em fase preliminar de planejamento[135]. O que culmina com o risco sistêmico enquanto possibilidade mais grave, como ocorreu na crise de 2008.

Analisando o ambiente de negócios sob o ponto de vista financeiro, entende-se que a regulação financeira pode ser dividida sob as funções de combate ao uso de ativos para atividades ilícitas, proteção do consumidor/investidor contra fraudes e abusos, e ainda garantir a integridade dos mercados e a estabilidade financeira, a intitulada regulação prudencial[136]. Assim, verifica-se que inexiste ao dispor deste investidor o Fundo Garantidor de Crédito brasileiro ou Fundo de Garantia de Depósitos português, assim como as demais normas e regras rígidas previstas para as instituições financeiras, que proporcionam inclusive maior segurança quanto à privacidade e proteção dos dados, que efetivamente podem se configurar como bancários, fiscais e econômicos, a ensejar devida proteção contra violações indevidas. Até mesmo o benefício da imutabilidade trazido pela *blockchain* se torna um problema em casos de erro, fraude ou roubo, não havendo dispositivos de *chargeback*[137].

Por sua vez, o mercado ainda se encontra sujeito a manipulações de preços por simples manifestações de figuras públicas[138]. A inexistência de mercado formalizado, sua abrangência ainda diminuta, ausência de lastro e de

---

132 Disponível em <URL:https://www.voitto.com.br/blog/artigo/sto-oferta-de-token-segura>, consult. 10.06.2020.

133 Como se sucedeu recentemente com a empresa FTX, em que houve decretação de falência e o seu ex-CEO foi preso acusado de fraude aos investidores.

134 Pirâmides financeiras são também chamadas de Esquema Ponzi, uma referência a Charles Ponzi, autor de gigantesca fraude na década de 1920. Tal possibilidade de rendimentos anormalmente altos se encontra presente quanto aos criptoativos, em que muitos investidores almejam lucros rápidos e por vezes irreais, sendo presas fáceis diante da multiplicidade de projetos lançados no mercado.

135 A exemplo do que aconteceu com o colapso do ecossistema UST Terra-Luna, *stablecoin* algorítmica que objetivava paridade com o dólar.

136 Otavio Yazbek, *Regulação do Mercado Financeiro e de Capitais*, Rio de Janeiro, Elsevier, 2007, pp. 180-189.

137 Christiana Mariani da Silva Telles, *Op. Cit*., p. 36. Trata-se o *chargeback* de disputa para reversão de transação em virtude de não reconhecimento por parte do titular, possibilidade existente no *e-commerce*.

138 As palavras de Elon Musk, CEO da Tesla, já foram capazes de proporcionar aumentos e quedas nas cotações de criptomoedas. Disponível em <URL:https://exame.com/

centralidade de informações diante da grande quantidade de plataformas, protocolos e sistemas a atuarem de forma simultânea e paralela, todos são fatores que dificultam a aferição dos preços de compra e venda dos ativos[139].

De outro modo, afora discussões sobre a natureza jurídica dos criptoativos, considerando que sua grande utilidade no contexto atual se configura como forma de investimento para os diversos *players* do mercado, importa aproximar as atividades desenvolvidas no mercado de capitais, principalmente pelas corretoras e administradoras das bolsas de valores, das atividades das *criptoexchanges*, enquanto intermediárias das plataformas de comercialização destes ativos, quer sejam estas caracterizadas como centralizadas ou descentralizadas[140].

Assim, mesmo diante dos benefícios trazidos pela tecnologia *blockchain* através da agilidade nas operações, principalmente em relação à janela de liquidação do sistema tradicional, bem como a desnecessidade de alguns intermediários e custodiantes para o bom funcionamento do sistema, verifica-se que os aspectos de pseudoanonimato e desintermediação próprios deste mercado podem ocasionar fragilidades. Isto não somente para o cometimento de ilícitos, tendo em vista a impossibilidade de segregação de valores em serviços de custódia e ausência de mecanismos de ressarcimento de prejuízos desenhados especificamente para situações envolvendo tais transações. Necessita-se, assim, repensar para o contexto das

future-of-money/criptoativos/o-impacto-das-publicacoes-de-elon-musk-no-mercado-de-criptomoedas/>, consult. 06.01.2022.

139 Conforme observam Tatiana Silveira Camacho e Guilherme Jonas Costa da Silva, "Criptoativos: Uma Análise do Comportamento e da Formação do Preço do Bitcoin", *in Rev. de Economia da Universidade Federal do Paraná* [Em linha], n° 68, Vol. 39, 2018, p. 22, disponível em <URL:https://revistas.ufpr.br/economia/article/view/67885>, consult. 24.12.2021, os preços dos criptoativos estariam relacionados a fatores internos, em particular à mineração, e a fatores externos relacionados aos aspectos mercadológicos, dentre eles podem ser destacados os processos regulatórios para proporcionar segurança aos investidores.

140 As plataformas centralizadas, enquanto intermediários em seu sentido tradicional, realizam a custódia dos ativos dos seus usuários, fornecendo carteiras virtuais e detendo chaves dos seus investidores, muito embora não tenham autorização para abertura de contas específicas para os seus clientes, ficando estes ativos em nome da própria plataforma, o que é um risco em diversos aspectos aos investidores, como furtos, falhas sistêmicas e bloqueios judiciais. As plataformas descentralizadas funcionam como *marketplaces*, ou seja, plataforma de negociação e trocas, não prestando serviço de compra e venda, supervisão e execução de transações, funcionando de maneira automatizada, geralmente através de *smart contracts* e *atomic swaps*. A identificação dos usuários se qualifica como problema de elevada monta neste segundo formato, porém verifica-se ainda ser percentualmente minoritária sua utilização no mercado (Giovana Treiger Grupenmacher, *As Plataformas de Negociação de Criptoativos: Uma análise comparativa com as atividades das corretoras e da Bolsa sob a perspectiva da proteção do investidor e da prevenção à lavagem dinheiro*, Dissertação (Mestrado em Direito), Escola de Direito da Fundação Getulio Vargas, São Paulo, 2019, pp. 57-58).

criptoexchanges a obrigação de melhor execução das ordens[141] e o sensível problema da *suitability*[142], conforme regras rigorosas instituídas por órgãos internacionais do mercado tradicional[143].

3.4. PROMOÇÃO DA HIGIDEZ DO SISTEMA FINANCEIRO E MONETÁRIO

Diante das consideráveis possibilidades de abrangência das atividades deste multifacetado setor, outro fator importante a se considerar é a afetação da estabilidade do mercado financeiro e monetário com a exposição dos bancos, públicos e privados, e outras empresas financeiras aos criptoativos[144], principalmente no universo das finanças descentralizadas ou DeFi[145], que grosso modo são aplicações de natureza baseadas em *blockchain* e concretizadas por meio de criptoativos. Assim, não necessitam de intermediários financeiros para verificação e fiscalização dos negócios realizados, diante da utilização de *smart contracts* e pretensa transparência e imutabilidade das transações.

---

141 Conforme Giovana Treiger Grupenmacher, *Op. Cit*., pp. 201-202, o tipo de ordem à mercado, em que o usuário não estabelece a exata cotação que quer transacionar o bem, encontra considerável dificuldade nestas plataformas quanto à comprovação de se aferir as melhores condições do mercado, tendo em vista que cada empresa tende a atuar de forma independente, utilizando-se do seu próprio ambiente negocial. Diferente do que ocorre em bolsas de valores, onde há cadeias de intermediários a promover tais regras e fiscalizar o seu cumprimento.

142 Segundo Julya Sotto Mayor Wellisch, *Mercado de Capitais: fundamentos e desafios*, São Paulo, Quartier Latin, 2018, p. 218, a *suitability*, enquanto categorização dos bens segundo o nível de risco que se encontre atrelado, divide-se nas atividades de regras de conduta voltadas à análise do perfil do investidor e classificação dos produtos, regras e procedimentos internos para a verificação da adequação do produto e dos mecanismos de atualização das informações dos usuários, bem como mecanismos de fiscalização e punição pelo seu não cumprimento. Principalmente após a crise de 2008, em contraposição ao *full disclousure*, verifica-se a necessidade de que o investidor seja acompanhado por intermediários que auxiliem na análise das melhores opções existentes no mercado, de acordo com o seu perfil e possibilidades, o que se encontra parcialmente prejudicado em plataformas centralizadas e severamente comprometido nas plataformas descentralizadas.

143 Como exemplo, Disponível em documento de 2013 da Organização Internacional de Valores Mobiliários (IOSCO) intitulado *Suitability Requirements With Respect to the Distribution of Complex Financial Products*, Disponível em <URL:https://www.iosco.org/library/pubdocs/pdf/IOSCOPD400.pdf>, consult. 06.01.2022.

144 O Conselho de Estabilidade Financeira, órgão internacional que monitora e faz recomendações sobre o sistema financeiro global, estabelecido após a cúpula do G20 em Londres, em abril de 2009, como sucessor do Fórum de Estabilidade Financeira, já demonstrou preocupação neste sentido: <URL:https://epocanegocios.globo.com/Economia/noticia/2019/05/epoca-negocios-avaliacoes-proativas-de-risco-de-moedas-digitais-sao-necessarias-diz-agencia-global.html>, consult. 10.06.2020.

145 Outros termos relacionados são *money legos*, *open finance* e *open source*, ao dispor que, em um ambiente proporcionado por plataforma descentralizada como a Ethereum, seria possível verificar e rastrear as transações, bem como pretensa independência de utilização do valor financeiro agregado.

Conforme Telles[146], tomando por base que o *bitcoin* (e de modo geral o restante das criptomoedas) não é emitido fisicamente nem pode ser impresso, o detentor deste bem possui, em realidade, uma chave digital privada sob a qual existe consenso de que possui autoridade sobre um determinado valor da mesma moeda, a qual, sob uma cotação flutuante, pode ser convertida em moeda fiduciária. Todavia, diferente das instituições financeiras, reguladas por controles internos rigorosos, sistemas de informação dotados de segurança e programas de integridade há muito implementados, não há tal obrigatoriedade na criptoeconomia, potencializada pela possibilidade de transferir valores sem contato pessoal e sem preocupação com as fronteiras internacionais.

De acordo com Ulrich[147] e sob a perspectiva da Trindade Impossível[148], estabeleceu-se para o *bitcoin* uma política monetária independente e liberdade total nos fluxos de capitais, entendendo que não há entidade que possa intervir em ciclos de alta e apreciação especulativa de modo a estabilizar a taxa de câmbio. Tendo em vista que investidores institucionais estão cada vez mais se interessando pelo mercado, inclusive com a diversificação de carteiras oferecidas pelas próprias instituições financeiras diante de potencial de rentabilidade e também por pressão da sua clientela, devem os agentes reguladores observar o fenômeno na perspectiva de que possível declínio financeiro desses ativos não tenha consequências desastrosas para o próprio sistema financeiro e monetário[149].

Importa registrar que não sendo consideradas juridicamente como instituições financeiras, muito embora tencionem prestar tipos análogos de serviços, tais plataformas de negociação de criptoativos não têm as mesmas obrigações a cumprir. Porém, também não podem usufruir dos mesmos benefícios, como a sistemática de resolução bancária prevista no ordenamento europeu, pelo que igualmente não estão sob supervisão e fiscalização de organismos internacionais como o Comitê de Supervisão Bancária da Basileia[150].

Inclusive fora aprovado pelo Grupo de Governadores do Banco Central e Chefes de Supervisão (GHOS) do Banco de Compensações Internacionais (BIS) um padrão prudencial universal sobre a exposição bancária a criptoativos, com limite de 2% nas reservas de criptoativos entre os bancos a ser

---

146 Christiana Mariani da Silva Telles, *Op. Cit*., p. 30.

147 Fernando Ulrich, *Op. Cit*., p. 77.

148 O mesmo autor define (ibidem) a Trindade Impossível como "um dilema em economia internacional que afirma que é impossível uma autoridade monetária adotar as três seguintes políticas simultaneamente: câmbio fixo, liberdade no fluxo de capitais e uma política de juros independente".

149 São muitas as instituições bancárias que já trabalham com criptoativos e/ou têm contato com a tecnologia *blockchain*, conforme se verifica em <URL:https://cryptoresearch.report/crypto-research/cryptocurrency-friendly-banks/>, consult. 15.04.2023.

150 BCBS, sigla de *Basel Committee on Banking Supervision* em inglês, trata-se de uma organização internacional de autoridades de supervisão bancária e financeira, que também emite recomendações sobre lavagem de dinheiro.

implementado a partir de 2025, conforme relatório intitulado "Tratamento prudencial de exposições a criptoativos".

Ainda que tal realidade seja considerada de baixa concretização em curto prazo, também não é inverossímil considerar a possibilidade de afetação da eficácia e eficiência de alguma política monetária a ser implementada por ente estatal caso o fluxo de recursos inseridos no mercado de criptoativos aumente de forma sensível. Essa situação poderia levar ao decréscimo do uso de moeda soberana e a diminuição da influência das taxas de juros de curto prazo, do controle sobre moeda e crédito e, consequentemente, na capacidade de implementar políticas anticíclicas que ajudem a proteger o nível de atividade e emprego domésticos diante de crises como a de 2008[151].

Sendo o mercado financeiro sistemicamente bastante complexo, baseado na confiança com que as instituições possuem e que as possibilita de se utilizarem dos valores depositados para promover a alavancagem de crédito, objetiva-se evitar a intitulada *corrida bancária* no setor de criptoativos, o que pode, considerando a dimensão relativamente pequena do setor, gerar um colapso que se espalhe e afete todo o seu sistema, atingindo como consequência o próprio setor financeiro tradicional e as economias locais que dele se utilizam. Por isso a importância de que haja regulação prudencial para a criptoeconomia[152].

3.5. RESPEITO À SUSTENTABILIDADE E RESPONSABILIDADE SOCIOAMBIENTAL

Por fim, embora não tenha sido expressamente incluído nas regulações estatais que se têm notícia, está a problemática do gasto energético demandado pelo processo de mineração dos criptoativos que se utilizam do protocolo de consenso *proof-of-work* (PoW), com destaque para o *bitcoin*, o que demanda máquinas avançadas de informática que trabalham incessantemente para validar transações e, com isso, serem os seus responsáveis gratificados com as recompensas[153]. Tanto que outros mecanismos de consenso foram criados, a exemplo do *proof-of-stake* (PoS) utilizado pelo *ethereum*, o qual se serve não do maior e mais potente poder computacional dos interessados, mas randomicamente sorteia aqueles que detêm maior quantidade daquele ativo para efetivar a respectiva mineração[154].

O consumo energético é de tal monta considerável que pode ser comparável ao que se utiliza em um país como a Argentina, que possui mais de 45

---

151 Cesar van der Laan, É crível uma economia monetária baseada em bitcoins? *Limites à disseminação de moedas virtuais privadas* [Em linha], Brasília, Núcleo de Estudos e Pesquisas/CONLEG/Senado, 2014, pp. 12-13, disponível em <URL:https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td163>, consult. 06.01.2022.

152 Giovana Treiger Grupenmacher, *Op. Cit*., p. 121.

153 Tatiana Silveira Camacho e Guilherme Jonas Costa da Silva, *Op. Cit*., p. 13.

154 Giovana Treiger Grupenmacher, *Op. Cit*., p. 34.

milhões de habitantes[155], bem como aparentemente exerceu influência direta nas quedas de energia sofridas na Venezuela. Neste caso, o governo local restou incapacitado de adicionar nova capacidade elétrica em face do alto uso advindo da mineração de *bitcoins* com o fim de driblar a hiperinflação[156].

Além disso, observa-se que, para aumentar a margem de lucro, os mineradores procuram se instalar em locais que se utilizam de matrizes energéticas mais baratas e excessivamente poluidoras. Assim, até 2020 a atividade se concentrava em sua maior parte na China, utilizando-se essencialmente de combustíveis fósseis. Todavia, alegando impedimento em atingir as metas de redução nas emissões de carbono, houve proibição de mineração de *bitcoin* no país[157]. Demonstrando a mesma preocupação, empresas já lançam *tokens* para compensação da "pegada de carbono"*[158]*, que são emissões de gases poluentes gerados pelas atividades produtivas das empresas.

Tratando-se de atividade transnacional, que não possui limite em fronteiras estatais e que pretende se consolidar globalmente, o ambiente regulatório também deve ser permeado por premissas básicas de supervisão e fiscalização das políticas de preservação ambiental, sustentabilidade e, especificamente neste tema, evitar alterações climáticas em decorrência do gasto excessivo de energia e da utilização de fontes reconhecidamente poluidoras como são os combustíveis fósseis.

Dentre os documentos internacionais em que os países se comprometeram com a responsabilidade socioambiental, destaque-se os Objetivos de Desenvolvimento Sustentável elencados na Agenda 2030, adotada por todos os Estados-Membros das Nações Unidas em 2015, que define as prioridades e aspirações do desenvolvimento sustentável para 2030 e procura mobilizar esforços globais à volta de um conjunto de objetivos e metas comuns.

Destes objetivos, releva salientar o de número 13, relacionado à Ação Climática, com vistas a melhorar a educação, aumentar a conscienciali-zação e a capacidade humana e institucional sobre medidas de mitigação, adaptação, redução de impacto e alerta precoce no que respeita às alterações climáticas[159]. Liga-se, portanto, ao consumo consciente e limpo de energia elétrica. Assim se deve pautar também o setor de criptoativos, que,

---

155 Conforme notícia a seguir, que utilizou dados da Universidade de Cambridge: <URL:https://www.bbc.com/news/technology-56012952>, consult. 06.01.2022.

156 Disponível em <URL: https://www.startse.com/noticia/nova-economia/tecnologia-inovacao/bitcoin-meio-ambiente-2018>, consult. 06.01.2022.

157 Disponível em <URL:https://www.seudinheiro.com/2021/bitcoin/bitcoin-mineracao-criptomoedas-china-eua/>, consult. 06.01.2022.

158 Como exemplos, cite-se MCO2 e o BITH11.

159 Disponível em <URL:https://unric.org/pt/objetivo-13-acao-climatica/>, consult. 06.01.2022.

enquanto ambiente inovador, há que se obrigar a cumprir requisitos mínimos de sustentabilidade global[160].

4. SITUAÇÃO DA REGULAÇÃO ESTATAL ATUAL

Tomando por base os problemas identificados no comércio de criptoativos, identificam-se propostas de autorregulação dos próprios *players* do mercado, como ocorre com o Código de Conduta e Autorregulação apresentado pela Associação Brasileira de Criptoeconomia (ABCRIPTO), acompanhado pelo "Manual de Boas Práticas em Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo para Exchanges brasileiras" [161]. Todavia, em que pese os ganhos de confiança e credibilidade de tais iniciativas[162], a obrigatoriedade se resume apenas àquelas empresas associadas, o que impossibilita a padronização de condutas e regulação em um ambiente transnacional.

Por isso, diante da necessidade de regulação da criptoeconomia em seus respectivos territórios soberanos, diversos países já dispuseram de alguma forma acerca do ambiente dos criptoativos[163]. Neste momento, selecionam-se os que se considera serem os mais importantes ao entendimento do tema, tanto no que concerne à proeminência do Estado como ao pioneirismo nos estudos regulatórios, demonstrando-se o estado da arte relacionado e a possibilidade, conforme se verificará adiante, de evolução do formato de regulação até então existente[164]. Para tanto, desde os extremos

---

160 Para conferir visão interessante acerca de como a tecnologia *blockchain* pode impactar positivamente no impacto ambiental, social e econômico, conferir trabalho do World Economic Forum intitulado "Guidelines for Improving Blockchain's Environmental, Social and Economic Impact", disponível em <URL:https://www.weforum.org/reports/guidelines-for-improving-blockchain-s-environmental-social-and-economic-impact/>, consult. 15.04.2023.

161 Disponível em <URL:https://www.abcripto.com.br/_files/ugd/55dd41_6a8e32790b5a40a08478fabdf373c4d3.pdf> e <URL:https://www.abcripto.com.br/_files/ugd/55dd41_206786481fc84485817e8d906b54b241.pdf>, consult. 26.01.2022.

162 Neste documento, elencam-se como condutas éticas com as quais estão comprometidos todos os associados: (i) livre concorrência, prevenção a fraudes e lavagem de dinheiro; (iii) prevenção e combate à corrupção; (iv) controle de informações e confidencialidade; (v) conformidade com as leis (Dayana de Carvalho Uhdre, *Op. Cit*., p. 192).

163 Para maiores informações especificamente acerca da regulação das criptomoedas pelo mundo, confira-se: The Law Library of Congress, "Regulation of Criptocurrency around the world. Report. Global Legal Research Center**"** [Em linha], Nov. 2021, disponível em <URL:https://tile.loc.gov/storage-services/service/ll/llglrd/2021687419/2021687419.pdf>, consult. 26.01.2022, e PwC, "PwC Global Crypto Regulation Report 2023" [Em linha], PwC, 2022, disponível em <URL:https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/pwc-global-crypto-regulation-report-2023.pdf>, consult. 30.03.2023.

164 Indica-se, para o contexto tributário, documento comparativo intitulado *PwC Annual Global Crypto Tax Report 2020*. Disponível em <URL:https://www.pwchk.com/en/research-and-insights/fintech/pwc-annual-global-crypto-tax-report-2020.pdf>, consult. 28.02.2022.

de proibição na China e legalização em El Salvador, passando pelos Estados Unidos da América e Venezuela no continente americano, por Suíça, Malta e Liechtenstein no continente europeu e por Japão e Singapura no continente asiático, chega-se ao comparativo entre o que existe no Brasil e em Portugal[165].

4.1. ENTRE A PROIBIÇÃO NA CHINA E A LEGALIZAÇÃO EM EL SALVADOR

Para se concluir e demonstrar a divergência de tratamento pelos diversos países acerca da matéria, basta verificar o tratamento jurídico contraditório espelhado entre China e El Salvador, percebendo-se desde a proibição de mineração e transações com criptomoedas até a introdução do *bitcoin* como moeda oficial de um país, o que ocorreu quase simultaneamente no mês de setembro de 2021.

Desde maio do referido ano que a China já havia proibido as instituições financeiras de ter qualquer tipo de negócio envolvendo criptomoedas, embora continuasse a existir liberdade para ser utilizada por pessoas a título individual[166], bem como havia proibido a mineração de *bitcoin* sob a justificativa de impedimento de serem atingidas as metas de redução de emissões de carbono[167].

Todavia, em comunicado de 24 de setembro de 2021, o Banco Popular da China divulgou memorando proibindo todas as transações com criptomoedas, ou seja, tornando atividades financeiras ilegais as transações comerciais vinculadas a moedas virtuais e que envolvam derivados de criptomoedas, bem como venda de *tokens* e arrecadação de fundos ditos ilegais. Tudo sob a justificativa de que tais atividades estariam ligadas a atos ilícitos como esquemas de pirâmide, lavagem de dinheiro e fraudes[168].

---

165 Para tanto, escuda-se inicialmente da doutrina de Dayana de Carvalho Uhdre, *Op. Cit*., pp. 127-154, Guilherme Campos Maia, *Op. Cit*., pp. 17-46, Christiana Mariani da Silva Telles, *Op. Cit*., pp. 80-104, e Joana Alexandre Giraldes Vieira Luz, *Regulação e Criptomoedas*, Dissertação (Mestrado em Direito), Universidade de Lisboa, Lisboa, 2020, pp. 17-39, tendo em vista tratarem de forma comparativa as regulações existentes, com vistas a elucidar as diferenças de entendimento.

166 Disponível em <URL:https://pplware.sapo.pt/internet/china-proibe-criptomoeda-em-bancos-e-sistemas-de-pagamento/> e <URL:https://www.reuters.com/technology/chinese-financial-payment-bodies-barred-cryptocurrency-business-2021-05-18/>, consult. 10.06.2021.

167 Embora se especule que tal estratégia possa se configurar como uma tentativa de o *yuan* digital, atualmente o projeto de CDBC mais bem desenvolvido do mundo, tornar-se a principal criptomoeda do mundo, ainda que o seu uso se reduza atualmente ao cenário doméstico chinês. Para mais informações: Joana Alexandre Giraldes Vieira Luz, *Op. Cit*., pp. 32-33.

168 Confira-se em: <URL:https://g1.globo.com/economia/noticia/2021/09/24/banco-central-da-china-declara-ilegais-todas-as-transacoes-com-criptomoedas.ghtml> e <URL:https://criptonizando.com/investidores-institucionais-veem-a-ultima-proibicao-da-china-como-oportunidade/>, consult. 26.01.2022.

De forma diametralmente oposta, El Salvador aprovou lei para adotar *bitcoin* como moeda de curso legal, sendo o primeiro no mundo a aceitá-la oficialmente ao obrigar qualquer agente econômico ao seu recebimento como forma de pagamento, exceto aquele que por fato notório e de maneira evidente não possua tecnologia para fazê-lo[169].

Assim, no dia 7 de setembro de 2021 entrou em vigor a intitulada *Ley Bitcoin*, após aprovação pela Assembleia Legislativa de El Salvador de proposta apresentada pelo presidente Nayib Bukele, que tem como objeto pioneiro a regulação do *bitcoin* como moeda de curso legal, irrestrito, com poder liberatório, ilimitado em qualquer transação e a qualquer título que as pessoas naturais ou jurídicas, públicas ou privadas, requeiram realizar[170].

Para tanto, fora previsto que o tipo de câmbio entre o dólar americano e o *bitcoin* seria estabelecido livremente pelo mercado, utilizando-se contabilmente o dólar como moeda de referência. Assim, possibilitou-se que todo preço possa ser expresso em *bitcoin* e todas as contribuições tributárias possam ser assim quitadas, obrigando-se a todo agente econômico aceitá-lo como forma de pagamento quando oferecido por quem adquire bem ou serviço, excetuando-se quando, por fato notório e de maneira evidente não se tenha acesso às tecnologias que permitam executar tais transações. Como meio de proporcionar a adoção pela população, o governo criou a carteira digital Chivo enquanto ecossistema de utilização.

Objeto de elogios dos entusiastas do uso da tecnologia *blockchain* e dos criptoativos de forma geral, a legislação também é matéria de críticas quanto à adoção do *bitcoin* como moeda de curso legal, a exemplo do Fundo Monetário Internacional[171]. Mesmo considerando que neste curto espaço de tempo de vigência da lei houve considerável desvalorização da criptomoeda[172] e que a maioria da população não a usa em suas transações corriqueiras[173], há que se aguardar por mais tempo a realidade local para se fazer um

---

169 Verifique-se em: <URL:https://g1.globo.com/economia/noticia/2021/06/09/congresso-de-el-salvador-aprova-lei-para-adotar-bitcoin-como-moeda-de-curso-legal.ghtml>, consult. 10.06.2021.

170 Confira-se a lei em: <URL:https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/27F0BD6F-3CEC-4F52-8287-432FB35AC475.pdf>, consult. 26.01.2022.

171 No dia 25 de janeiro de 2022, o FMI alertou El Salvador no sentido de que a adoção do *bitcoin* confere grande risco à estabilidade e integridade financeira do país, requerendo a revogação da legislação. Confira-se em: <URL:https://expresso.pt/economia/fmi-exige-que-el-salvador-deixe-de-usar-bitcoin-como-moeda-de-curso-legal/>, consult. 26.01.2022.

172 O governo de El Salvador possui o total de 1.801 *bitcoins* no seu tesouro nacional, acumulando perda considerável do seu valor no período. Disponível em <URL:https://exame.com/future-of-money/investimento-milionario-de-el-salvador-em-bitcoin-ja-perdeu-26-do-valor/>, consult. 26.01.2022.

173 Até o momento, segundo dados de pesquisa do Instituto Universitário de Opinião Pública (IUOP), da Universidad Centroamericana José Simeón Cañas, de El Salvador, 74% da população não fez uso da criptomoeda. Conforme se verifica em: <URL:https://www.

diagnóstico técnico-científico das consequências legais e econômicas da institucionalização salvadorenha.

4.2. SOBREPOSIÇÃO DE REGRAS E ÓRGÃOS NOS ESTADOS UNIDOS E O PETRO VENEZUELANO

Nos Estados Unidos, que sempre tem o poder de irradiar e influenciar seus entendimentos mundo afora, além das propostas legislativas que objetivam normatizar e regular aspectos sobre criptoativos e tecnologia *blockchain*[174], o que existe é verdadeira sobreposição normativa de competência de órgãos reguladores, traduzindo-se em regulamentação multilateral para aplicação das leis federais e regulamentos já existentes.

Enquanto o *State Banking* tenta regulamentar as trocas de criptomoedas e dinheiro, o *Internal Revenue Service* (IRS) dá conta do tratamento destes criptativos como sujeitas ao ganho de capital (*capital gains tax*) diante do seu tratamento como propriedade[175], descartando, portanto, sua qualificação como moeda estrangeira nesta jurisdição[176].

Por sua vez, a *Treasury's Financial Crimes Enforcement Network* (FinCEN), que tem como missões a proteção do sistema financeiro e o combate à lavagem de dinheiro, tenta aplicar a *US Bank Secrecy Act*[177] (BSA) às trocas de criptomoedas com vistas à detecção do delito de lavagem de dinheiro, bem como o regime *Anti-Money Laundering* (AML) ao universo dos criptoativos[178]. Registre-se que, de acordo com Telles[179], apenas *exchanges*, administradores e anonimizadoras são considerados *money transmitters* e, portanto, sujeitos às disposições do BSA e à regulação do FinCEN[180], como obrigação

cnnbrasil.com.br/business/74-da-populacao-de-el-salvador-nao-usou-bitcoin-desde--que-moeda-foi-oficializada/>, consult. 26.01.2022.

174 São cerca de 21 propostas legislativas em tramitação federal nos Estados Unidos com objetivo de normatizar aspectos dos criptoativos e da tecnologia *blockchain*. Para maiores informações, v. Dayana de Carvalho Uhdre, *Op. Cit*., p. 128.

175 Para mais informações sobre tributação pelo imposto de renda na modalidade de ganho de capital nos EUA, bem como diferenças quanto à legislação brasileira, indica-se Marcos Aurélio P. Valadão e Valcir Gasse, *Tributação nos Estados Unidos e no Brasil* [Em linha], São Paulo, Almedina, 2020, pp. 110-170, disponível em <URL:https://integrada.minhabiblioteca.com.br/#/books/9788584936267/>, consult. 30.01.2022.

176 Neste sentido, conforme disposto em Liziane Angelotti Meira, Fillipe Soares Dall'ora e Hadassah Laís S. Santana, *Op. Cit*., p. 350, o recebimento de pagamento em moeda virtual deve ser tributado como pagamento feito com bens, ao passo que a mineração enquanto atividade de produção de moedas deve ser tributada enquanto rendimento de trabalho autônomo.

177 Lei de sigilo bancário americano.

178 Para mais informações, Disponível em Joana Alexandre Giraldes Vieira Luz, *Op. Cit*., p. 26.

179 Christiana Mariani da Silva Telles, *Op. Cit*., pp. 94-95.

180 Considerando *exchanges* como aqueles que compram e vendem criptomoedas e administradores como mineradores que tendem a colocar criptomoedas em circulação,

de registro, comunicação de transações suspeitas, instituição de programa antilavagem de dinheiro efetivo e aplicação de ferramentas de *Know Your Client* (KYC). Por fim, ressalte-se a aplicabilidade de tais regras às plataformas sem presença efetiva no país, desde que transacionem em sua totalidade ou em parte substancial no seu território (ibidem, p. 97).

Em outra seara, há embate entre a *Securities and Exchange Commission* (SEC) e a *Commodity Futures Trading Comission* (CFTC), tendo em vista a possível caracterização dos criptoativos entre *security tokens* ou *commodities*, o que possibilitaria a aplicação do regime de investimento enquanto regramento destinado à proteção de investidores potencialmente aplicáveis e os mercados financeiros. Sobre a SEC, entendendo pela aplicação da *Security Law* na tecnologia *blockchain*[181], utiliza-se do teste de Howey[182] para identificar se uma oferta de *token* apresenta natureza jurídica de valores mobiliários, já possuindo entendimento firmado pelo não cabimento nos casos de criptomoedas como *bitcoin* e *ethereum*[183]. Todavia, verifica-se ostensiva atuação deste órgão[184], o que vem causando pressão regulatória no território e, possivelmente, proporcionará atração de empresas para outras jurisdições, nomeadamente Europa e Ásia. A CFTC, por sua vez, já trata alguns criptoativos como o *bitcoin* enquanto *commodities*, atraindo sua supervisão e sujeição ao *Commodity Exchange Act* (CEA).

Por fim, para configurar a diversidade de entendimentos legislativos existentes, até mesmo o *New York State Department of Financial Services* (NYDFS) definiu a exigência de licença específica para qualquer pessoa residente no Estado de Nova York ou que queira transacionar na sua extensão territorial, chamado *BitLicence*. Este contexto obrigacional ocasionou a retirada de diversas empresas para outros Estados americanos, que passaram a utilizar como parâmetro regulatório o modelo elaborado pela associação

não estão sujeitas a tais normas os simples usuários e os mineradores que objetivam exclusivamente a troca desses ativos por bens ou serviços.

181 Para mais informações, indica-se Guilherme Campos Maia, *Op. Cit*., p. 19.

182 Conforme Dayana de Carvalho Uhdre, *Op. Cit*., p. 129, e Guilherme Campos Maia, *Op. Cit*., pp. 20-22, a aplicação desse teste, com o fim de identificação se um ativo detém natureza de valor mobiliário, reverte-se em três elementos cumulativos: a) investimento de recursos, seja por dinheiro, criptomoedas, entrada em indústria ou doações; b) empreendimento coletivo, em que os *tokens* devem ser fungíveis, o emissor deve agrupar os fundos arrecadados das vendas e deve usá-los para desenvolver o projeto; c) com expectativa de obtenção de lucros (que deve sobrepor-se ao potencial uso do bem) que decorram de esforços de terceiros (nunca do próprio investidor).

183 Não há aplicabilidade quando ao segundo requisito do *Howey Test*.

184 Sobre o assunto: <URL:https://exame.com/future-of-money/acao-da-sec-contra-gigantes-cripto-mostra-incerteza-juridica-do-setor-nos-eua-e-deve-afetar-mercado/>, <URL:https://exame.com/future-of-money/sec-notifica-coinbase-violacao-leis-eua/> e <URL:https://portaldobitcoin.uol.com.br/para-onde-vao-as-empresas-de-criptomoedas-com-a-pressao-dos-reguladores-opiniao/>, consult. 15.04.2023.

americana *Uniform Law Commission* (ULC) denominada *Virtual Currency Business Act* (VCBA).

Registre-se que, assim como ocorre com os *payment tokens*, tanto os *utility* como *security tokens* também são tributados segundo o regime de ganhos de capital, tendo em vista a aplicabilidade do *Howey Test* quanto ao preenchimento da expectativa de lucro diante da especulação do valor de mercado desses ativos[185].

Ainda no continente americano, destaque-se o cenário vivenciado na Venezuela, em que, diante da perspectiva de hiperinflação, colapso do sistema financeiro e de subsídio governamental no fornecimento de eletricidade, o próprio ente estatal, além de proporcionar ambiente favorável de mineração, foi pioneiro e instituiu em 2017 o Petro enquanto moeda digital e soberana emitida pela sua República Bolivariana[186], respaldada por *commodities*[187].

Justifica-se o uso massivo de criptomoedas na Venezuela em razão das sanções impostas pelos Estados Unidos, da impossibilidade de realização de transações em dólares, da demora na concretização de transações financeiras no sistema *swift*, da alternativa como poupança em face do bolívar soberano e ainda como meio atrativo de envio de remessas dos cidadãos que migraram do país[188].

Diante disto, foi proporcionada regulação através de decretos e criação da *Superintendencia Nacional de Criptoactivos y Actividades Conexas* (SUNACRIP) como órgão autônomo responsável pela regulação e supervisão do setor, proporcionando segurança e garantia legal para investimentos e trocas comerciais. Destaque-se a obrigação de registro de informações referentes às atividades de mineração e de reparação de serviços relacionados aos seus equipamentos, bem como aos que se dedicarem à venda, ICO's, operadores de caixas automáticos e fundos de inversão de criptomoedas[189].

Por fim, ressalte-se que, em que pese a legislação venezuelana não seja clara, a doutrina entende que as operações e transações envolvendo cripto-

---

185 Conforme Guilherme Campos Maia, *Op. Cit*., p. 23.

186 Conforme Joana Alexandre Giraldes Vieira Luz, *Op. Cit*., p. 23, a moeda pode ser usada para compra de *commodities*, pagar impostos e serviços públicos na Venezuela, bem como bens e serviços de uso particular, envio de encomendas e de remessas pela plataforma Petroapp. Para mais informações: <URL: https://petro.gob.ve/en/>, consult. 30.01.2022.

187 Conforme o *whitepaper* (p. 7), o petróleo representa 50% desse valor, seguido pelo ouro e ferro com 20% cada e diamante representando os outros 10%. Desse modo, tecnicamente deve ser considerada uma CBDC. Disponível em <URL:https://petro.gob.ve/static/images/petro-whitepaper.pdf>, consult. 30.01.2022.

188 De acordo com o Índice de Adoção de Criptografia Global 2020, elaborado pela empresa Chainalysis, a Venezuela é o terceiro país no mundo que mais realiza transações com criptomoedas. Confira-se em: <URL:https://www.brasildefato.com.br/2020/10/14/com-petro-venezuela-e-terceira-no-ranking-mundial-de-transacoes-em-criptomoedas>, consult. 30.01.2022.

189 Para mais informações sobre os decretos existentes e sua abrangência, confira-se Joana Alexandre Giraldes Vieira Luz, *Op. Cit*., pp. 23-25.

moedas estariam sujeitas ao imposto sobre ganhos de capital[190], ao passo que recentemente restou estabelecida legislação a tratar sobre medidas antilavagem de dinheiro e de combate ao financiamento do terrorismo[191].

4.3. EXPERIÊNCIAS EUROPEIAS EM SUÍÇA, MALTA E LIECHTENSTEIN

Na Europa, destacam-se as pioneiras iniciativas da Suíça, Malta e Liechtenstein, os quais, conhecidos como históricos paraísos fiscais, não por acaso tiveram interesse em, da sua maneira, regular o ambiente dos criptoativos e atrair investimentos. Por isso, são considerados *crypto-friendly*, diante da regulamentação considerada atrativa para os negócios envolvendo criptoativos. Registre-se que Crypto Valley (região localizada primeiramente em Zug e que hoje ocupa áreas de Liechtenstein[192]), Ethereum Foundation e Libra Association (criadoras respectivamente das criptomoedas que levam os mesmos nomes) têm suas sedes na Suíça.

Partindo de Uhdre[193], em fevereiro 2018 a Suíça publicou guia (*ICO Guideline*) para informar aos usuários como a Autoridade Suíça de Supervisão do Mercado Financeiro (FINMA) aplicaria a legislação do mercado financeiro neste âmbito, com análise casuística das circunstâncias a cada hipótese analisada diante da ausência de regulamentação específica, jurisprudência ou doutrina consistente.

Assim, com base na função econômica ou finalidade relacionada ao *token* emitido, a FINMA diferencia as categorias entre pagamento (*payment*), de valores mobiliários (*security*)[194] e utilitário (*utility*)[195], não descartando tam-

---

190 Conforme Gabriel Alejandro Chirinos, "Regulación y Tributación en el Mercado de Criptoactivos, una Perspectiva de Derecho Comparado", *in Rev. de la Facultad de Derecho Montevideo* [Em linha], n° 48, 2020, p. 29, disponível em <URL:https://perma.cc/3TNK-8ZEZ>, consult. 30.01.2022.

191 *Normas Relativas a la Administración y Fiscalización de los Riesgos Relacionados con la Legitimación de Capitales, el Financiamiento del Terrorismo y el Financiamiento de la Proliferación de Armas de Destrucción Masiva, Aplicables a los Proveedores de Servicios de Activos Virtuales y a las Personas y Entidades que Proporcionen Productos y Servicios a través de Actividades que Involucren Activos Virtuales, en el Sistema Integral de Criptoactivos*. Disponível em <URL:https://perma.cc/HW5T-D37B>, consult. 30.01.2022.

192 Termo cunhado em alusão ao Silicon Valley, lar de gigantes da tecnologia localizado nos Estados Unidos da América, Crypto Valley atrai diversas empresas do setor de criptoativos, proporcionando ambiente de inovação e de desenvolvimento de negócios e soluções nesta área. Mais informações em: <URL:https://members.cryptovalley.swiss/page/why-switzerland>, consult. 11.02.2022.

193 Dayana de Carvalho Uhdre, *Op. Cit*., pp. 142-145.

194 Registre-se ainda diferenciação dos *security tokens* entre *investment tokens* (títulos que atribuem rendimento de capital ao seu titular com base na atividade concretizada pelo emissor, possuindo o lucro como finalidade social e econômica) e *asset-backed tokens* (títulos que representam ativos, quantificados diretamente de acordo com o valor desse ativo subjacente), conforme se vislumbra em Guilherme Campos Maia (2019, p. 15).

195 Classificação ainda hoje usual para diferenciar as categorias de criptoativos.

bém o hibridismo e tornando obrigatória a identificação dos proprietários dos dois primeiros tipos em razão da legislação anti-branqueamento de capitais e de financiamento ao terrorismo. Por sua vez, especificamente quanto aos *tokens* de ativos, reveste-se importância a mitigação da assimetria de informações através de negociação justa, confiável e com preços eficientes.

Em seguida, fora aprovada em setembro de 2020, com efeito no primeiro trimestre de 2021, a *Blockchain Act*, que empreendeu alterações a diplomas já existentes de alcance federal. Destaca-se a introdução de títulos não certificados com base em DLT na legislação de títulos civis suíços, a criação de nova categoria de licença independente e específica para instalações de negociação DLT, e ainda a possibilidade de terceiro requerer a segregação de ativos digitais em caso de falência de custodiante de *tokens*.

Em relação a Malta, instituiu em 2018 três leis com escopo de regulamentação do setor de forma ampla, trazendo segurança jurídica a quem empreende no setor: *Virtual Financial Assets Act* (VFAA ou Lei de Ativos Digitais), *Malta Digital Innovation Authority Act* (MDIA ou Lei da Autoridade de Inovação de Malta) e *Innovative Technology Arrangements and Services Act* (ITAS ou Lei de Serviços e Arranjos Tecnológicos).

Conforme se verifica resumidamente de Uhdre[196], a VFAA é de observância obrigatória dos agentes do setor, estabelece requisitos mínimos para que uma ICO possa ser considerada regular, e diretrizes a serem seguidas por emissores de *tokens*, intermediários e prestadores de serviços. A MDIA prevê a forma de regulamentação do setor de criptomoedas e de tecnologias em *blockchain*. Por fim, a ITAS trata do registro de prestadores de serviços de tecnologias e certificação de plataformas DLT.

Acerca do enquadramento jurídico de um ativo DLT, verifica-se em Maia[197] elucidativa classificação de Malta entre *eletronic money*, *financial instrument* (FI, que ainda se divide entre *transferable securities* e *other financial instruments*), *virtual token* (VT) e *virtual financial asset* (VFA). Todavia, em seu enquadramento fiscal, a tributação dos criptoativos considera apenas duas categorias, quais sejam, *coins* e *tokens*. Por sua vez, os últimos são divididos ainda em *financial tokens* e *utility tokens*.

As *coins* se relacionam aos VFA e, por consequência, às criptomoedas, em que apenas são tributados os ganhos derivados de atividade econômica ou comercial enquanto *ordinary income*, tendo em vista que esta categoria não se enquadra na tributação de *capital gains*. Já os *financial tokens*, subsumidos aos FI em sentido jurídico e aos *security tokens* e os ativos *tokenizados* no sentido funcional, podem ter tributados seus rendimentos como *ordinary income* caso derivados de atividade profissional ou comercial, ou como *capital gains* em casos específicos. Por fim, os *utility tokens*, mesmo se aproximando dos tradicionais *tokens* de mesma categoria funcional, di-

196 Dayana de Carvalho Uhdre, *Op. Cit*., pp. 146-147.

197 Guilherme Campos Maia, *Op. Cit*., pp. 24-28.

ferenciam-se por se restringirem às transações na plataforma emissora ou em rede limitada delas, tributando-se do mesmo modo que as *coins*.

Em relação a Liechtenstein, conforme Uhdre[198] vigora desde janeiro de 2020 a lei intitulada *Token and Trusted Technology Service Provider Act* (TVTG), convencionada como *Liechtenstein Blockchain Act*. De forma inovadora e interessante, esta legislação, sincronizando o mundo físico ao virtual, autoriza a conversão de qualquer ativo ou direito em *tokens* através do *Token Container Model* (TCM), modelo em que se podem acondicionar direitos e ativos das mais variadas naturezas, preenchido unicamente pelo código digital, como no caso das criptomoedas.

O foco é a possibilidade de diferenciar o bem físico e o ativo *tokenizado* correspondente, ou seja, o direito e a tecnologia subjacente, em que o primeiro poderá ter sua propriedade transferida sem necessidade de mudança de localização, apenas com a tradição do segundo. Assim, garante-se a integridade da correspondência entre mundo físico e virtual através de responsável devidamente licenciado, com o fim de manter a sincronia de ambos.

4.4. VISÃO ASIÁTICA EM SINGAPURA E NO JAPÃO

Visualizando-se o continente asiático, optou-se por especificar as propostas legislativas levadas a cabo em Singapura e no Japão, diante da relevância dos países e da construção e perspectiva regulatória perseguida por ambos.

Acerca de Singapura, trata-se do país mais competitivo do mundo conforme dados do Fórum Econômico Mundial apresentados no *Global Competitiveness Report* de 2019, período anterior ao início da pandemia, baseando-se em termos de infraestrutura, saúde, funcionamento do mercado de trabalho e desenvolvimento do sistema financeiro[199]. Também há que se destacar o baixo percentual de impostos a serem pagos por seus cidadãos e empresas, o que impacta diretamente na atração da criptoeconomia.

Baseando-se na doutrina de Maia[200] e considerando que não existe no país incidência tributária sobre ganhos de capital, tal se reflete no enquadramento jurídico dos *tokens*, os quais só têm sua oferta ou emissão regulada se forem qualificados como *capital market products*[201] pela *Securities and*

198 Dayana de Carvalho Uhdre, *Op. Cit*., pp. 148-151.

199 Disponível em <URL:https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf>. Na edição especial de 2020, que se baseou na perspectiva de como os países estão se saindo no caminho da recuperação econômica, vislumbra-se que Singapura também é destaque em diversos aspectos, figurando, por exemplo, entre os dez principais países em adoção de tecnologia da informação e comunicação (TIC), competências digitais e quadro ou marco jurídico digital. Verifica-se em: <URL:https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2020.pdf>, consult. 11.02.2022.

200 Guilherme Campos Maia, *Op. Cit*., pp. 17-19.

201 Considerados instrumentos financeiros e, para o presente trabalho, enquadrados na categoria de *security tokens*.

Futures Act (SFA). Tudo de acordo com o *Guide to Digital Token Offerings* publicado em 2017 pela *Monetary Authority of Singapore* (MAS). Portanto, os *payment* e os *utility tokens* não possuem previsão legal no país.

Tratando-se do enquadramento fiscal destes criptoativos, baseando-se na regulação instituída pela *Inland Revenue Authority of Singapore* (IRAS), embora a mais-valia obtida com a comercialização de *payment* e *utility tokens* seja tributável, apenas as atividades de *trading*[202] serão efetivamente tributadas a título de imposto de renda (*income tax*), pois que, caso contrário, não haverá tributação por estar enquadrado o lucro no regime de *capital gains*. Em relação aos *security tokens*, sendo considerados *capital market products*, o rendimento resultante da comercialização desses bens é considerado como investimento pessoal, que, por sua vez, enquadrado como *capital gains*, não será tributado.

Por fim, caso as empresas sediadas no país tiverem como negócio principal a transação de tais *tokens*, bem como aceitarem criptomoedas como meio de pagamento (que, em realidade, constituirá como meio de troca), estarão sujeitas à tributação. Demonstram-se, assim, importantes incentivos para o mercado de criptoativos no território.

Sobre o Japão, um dos países mais evoluídos no que diz respeito à regulação de criptomoedas[203], foram aprovadas legislações desde 2016 que trazem maior segurança para o desenvolvimento de negócios com criptoativos. Inicialmente a Lei das Fintechs, que entrou em vigor em 1° de abril de 2017, proporcionou no âmbito das moedas digitais alterações na *Payment Service Act* (PSA - Lei sobre Arranjos de Pagamento) e na Lei de Prevenção de Movimentação de Recursos Provenientes do Crime (a lei antilavagem japonesa).

Quanto à primeira (PSA), conceituou-se moedas virtuais em seu art. 2º, parágrafo 5º, inciso (i)[204].Também se destaque do art. 2°, parágrafo 7°, a descrição e regulação das atividades enquadradas na prestação de serviços

---

202 Os critérios definidos para a existência de *trading* se revestem na natureza do ativo a ser comercializado, duração do período de compra e venda, frequência das transações, trabalho suplementar, circunstâncias da realização, elemento volitivo, financiamento e outros definidos pela IRAS (Guilherme Campos Maia, *Op. Cit*., p.18).

203 Conforme Joana Alexandre Giraldes Vieira Luz, *Op. Cit*., p. 30.

204 Como se verifica em Eduardo Mesquita Kobayashi, "Regulação de criptoativos no Japão - Marco regulatório, jurisprudência e doutrina", *in Rev. de Direito Público da Economia – RDPE* [Em linha], n° 67, ano 17, 2019, p. 118, Belo Horizonte, Fórum, pp. 115-136, disponível em <URL:https://www.researchgate.net/publication/338779262_Regulacao_de_criptoativos_no_Japao_-_Marco_regulatorio_jurisprudencia_e_doutrina_Cryptoassets_Regulation_in_Japan_-_Legal_framework_case_law_and_theory>, consult. 13.02.2022, doutrina esta que pode ser conferida para mais detalhes: "valor patrimonial (restritos aqueles registrados em dispositivo eletrônico ou outros meio eletrônicos, excluída moeda de curso forçado no Japão e câmbio internacional) que pode ser utilizado em relação a pessoas indeterminadas para o fim de pagamento na compra ou empréstimo de produtos, ou por serviços prestados, e que podem ser adquirido ou vendido para pessoas indeterminadas, podendo ser transferidos através de um sistema de processamento de dados eletrônicos".

das plataformas eletrônicas, ou de *exchanges* de moedas virtuais. Para estas prestadoras de serviços de *exchanges* legitimamente operarem, estão sujeitas à autorização do primeiro-ministro[205] e a requisitos mínimos para garantia da operação segura e desenvolvimento dos serviços. Assim, poderão atuar basicamente nos serviços de compra e venda dessas moedas virtuais diretamente dos usuários, na intermediação dessas transações sem a aquisição (chamado *matching*) e ainda nos serviços de administração dessas moedas enquanto custodiantes[206].

Quanto à lei antilavagem, foram criadas obrigações adicionais às *exchanges* com o objetivo de combate ao branqueamento de capitais e financiamento ao terrorismo, ao serem consideradas como "operadoras especiais", ou seja, potenciais veículos para transferência de recursos que tenham origem em atividades criminosas, conforme já estavam inseridos bancos, cooperativas de crédito, seguradoras e fundos de investimento[207]. Com isso, são previstos deveres de prevenção à lavagem de dinheiro (AML) e de identificação dos clientes (KYC), sobremaneira em transações com potenciais de risco e suspeitas de relação com delitos.

Já em maio de 2020 passou a vigorar proposta regulatória que alterou novamente a PSA, mas também a *Financial Instruments and Exchange Act* (FIEA - Lei de Instrumentos Financeiros e Câmbio), com regras aplicáveis pela *Financial Services Agency* (FSA - Agência de Serviços Financeiros), órgão ao qual é obrigatório o registro dos serviços de câmbio de moeda virtual, incluindo os fornecedores estrangeiros, que devem ter provedor de serviços com domicílio no Japão[208].

Através desta alteração, ficaram sob a supervisão da FSA as operações com derivativos de criptoativos e as ofertas iniciais de *tokens* de ativos (STO) ou de moedas (ICO), todos entendidos como instrumentos financeiros. Tais *tokens* não são considerados moedas virtuais (reguladas pela PSA), mas qualificados como direitos transferíveis registrados eletronicamente (ERTRs). Emitidos com a expectativa de lucro, estes ERTRs são enquadráveis sob a natureza de *security tokens* e, por isso, submetem-se à FIEA[209].

Além da alteração das terminologias moedas virtuais ou criptomoedas para criptoativos, consoante a linguagem de organismos internacionais, fo-

---

205 Dayana de Carvalho Uhdre, *Op. Cit*., p. 151.

206 Eduardo Mesquita Kobayashi, *Op. Cit*., p. 119.

207 Dayana de Carvalho Uhdre, *Op. Cit*., p. 152.

208 Conforme Joana Alexandre Giraldes Vieira Luz, *Op. Cit*., pp. 30-31, doutrina que se indica para mais informações sobre supervisão e auditoria das atividades por parte do *Cabinett Office Order* e do Primeiro Ministro.

209 Dayana de Carvalho Uhdre, *Op. Cit*., pp. 153-154. Para mais informações sobre as recentes alterações introduzidas, indica-se Katsuhiko Fujihira e Seth M. Graham, "Japanese Cryptocurrency Update: New Amendments to Crypto Asset Regulations Take Effect May 1" [Em linha], Abr. 2020, disponível em <URL://www.mofo.com/resources/insights/200423-japanese-cryptocurrency-update.html>, consult. 13.02.2022.

ram tomadas medidas para conceder maior proteção aos investidores em criptoativos que utilizem *exchanges* e custodiantes que operem no país. Como exemplos, a regulação das atividades de publicidade das plataformas digitais e a exigência de maior transparência no contrato com usuários[210]. Por fim, restou prevista a obrigação destas empresas de gerenciar os valores pertencentes aos usuários de forma separada dos fluxos de caixa, ou seja, utilizar de terceirização e métodos confiáveis de manutenção dos valores de seus clientes, como carteiras frias (*coldwallets*) e equivalentes. Caso não procedam, terão que manter fundos com valores de mesmo tipo e quantidade para reembolsá-los em caso de extravio e roubo dos montantes[211].

4.5. TRATAMENTO LEGAL EM PORTUGAL E NO BRASIL

Diferente dos países anteriormente listados, que vislumbraram na criptoeconomia a necessidade de regulação legal para estabelecimento de parâmetros firmes e homogêneos de enquadramento jurídico e fiscal, tanto em Portugal como no Brasil a legislação específica sobre o tema é recente, sendo alicerçada por manifestações e regulamentos de órgãos estatais.

Quanto a Portugal, destaque-se que tanto o Banco de Portugal como a Comissão de Mercado de Valores Mobiliários (CMVM) já emitiram comunicados e publicações ressaltando os riscos associados ao mercado[212]. Assim, com base em estudo do Banco Central Europeu de outubro 2012, intitulado *Virtual Currency Schemes*[213], em alerta da Autoridade Bancária Europeia de 12 de dezembro de 2013 direcionado aos consumidores sobre as ditas moedas virtuais[214]

---

210 Eduardo Mesquita Kobayashi, *Op. Cit*., p. 134.

211 Dayana de Carvalho Uhdre, *Op. Cit*., p. 153. Evita-se, assim, o que ocorreu com as empresas Mt. Gox e Coincheck, vítimas de roubos multimilionários, o que causou, inclusive, a falência da primeira, que era em 2013 e 2014 o maior intermediário de criptomoedas no mundo. Disponível em <URL:https://g1.globo.com/tecnologia/noticia/2014/02/mt-gox-entra-com-pedido-de-falencia-e-culpa-hackers-por-perda-de-bitcoins.html> e <URL:https://tecnoblog.net/noticias/2018/01/29/roubo-nem-coincheck-japao/>, consult. 13.02.2022.

212 Destaque-se, pela longevidade, comunicado da CMVM de 23.07.2018 acerca da qualificação jurídica dos tokens no contexto de lançamento de ICOs, disponível em <URL:https://www.cmvm.pt/pt/Comunicados/Comunicados/Pages/20180723a.aspx>, consult. 15.04.2023.

213 Disponível em <URL:https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, consult. 23.02.2022.

214 Disponível em <URL:https://www.eba.europa.eu/sites/default/documents/files/documents/10180/598420/30043572-6454-45f9-8e8a-13776cd752da/EBA_2013_01030000_PT_TRA%20Rev_Vinay.pdf?retry=1>, consult. 23.02.2022.

e ainda em parecer da Autoridade Bancária Europeia de 04 julho de 2014[215], o Banco de Portugal emitiu alerta em 03 de outubro de 2014[216].

Este documento, que é precedido pelo esclarecimento do Banco de Portugal sobre o *bitcoin* de 22 de novembro de 2013[217], foi ainda complementado pelo Banco de Portugal através da Carta Circular n.º 011/2015/DPG, de 10 de março de 2015[218], pela CMVM através do alerta aos investidores sobre *Initial Coin Offerings*, de 3 de novembro de 2017[219] e pelo Conselho Nacional de Supervisores Financeiros através de outro alerta aos consumidores novamente sobre moedas virtuais[220]. Em comum, todos destacam problemas como enorme volatilidade, ausência de proteção, falta de transparência, informação insuficiente, riscos de fraude ou de branqueamento de capitais e inadequação das "moedas virtuais" para a maioria dos fins. Tais orientações ainda persistem até o presente momento, demonstrando aparentemente o desestímulo aos interessados em investir nesta nova economia[221].

Em relação à legislação esparsa que fora aprovada e se encontra relacionada ao mercado de criptoativos[222], destacam-se a Lei 58/2020, de 31 de agosto, a Lei 79/2021, de 24 de novembro, e a recente aprovação do regime fiscal dos criptoativos pela Lei do Orçamento do Estado para 2023.

A primeira lei (Lei 58/2020) transpõe a Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio, que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e a Diretiva (UE) 2018/1673 do Parlamento Europeu e do Conselho, de 23 de outubro, relativa ao combate ao branqueamento de capitais através do di-

---

215 Disponível em <URL:https://clientebancario.bportugal.pt/pt-pt/publicacao/parecer-da-eba-sobre-moedas-virtuais>, consult. 23.02.2022.

216 Disponível em <URL:https://www.bportugal.pt/comunicado/alerta-aos-consumidores-para-os-riscos-de-utilizacao-de-moedas-virtuais>, consult. 23.02.2022.

217 Conforme se verifica em: <URL:https://www.bportugal.pt/comunicado/esclarecimento-do-banco-de-portugal-sobre-bitcoin>, consult. 23.02.2022.

218 Disponível em <URL:https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares/11-2015-dpg.pdf>, consult. 23.02.2022.

219 Disponível em <URL:https://www.cmvm.pt/pt/Comunicados/Comunicados/Pages/20171103a.aspx>, consult. 23.02.2022. Neste sítio se encontram igualmente disponíveis documentos oriundos da ESMA (Autoridade Europeia dos Valores Mobiliários e dos Mercados) emitidos a 13 de novembro de 2017 tratando sobre riscos para investidores e empresas quanto as ICO's.

220 Disponível em <URL:https://www.bportugal.pt/sites/default/files/anexos/comcnsf20180705.pdf>, consult. 23.02.2022.

221 Em 24 de fevereiro de 2021 o Banco de Portugal reitera os alertas aos consumidores sobre riscos associados aos ativos virtuais, utilizando nomenclatura mais atualizada e abrangente do que outrora utilizou. Disponível em <URL:https://www.bportugal.pt/comunicado/banco-de-portugal-reitera-alertas-aos-consumidores-sobre-riscos-associados-aos-ativos>, consult. 23.02.2022.

222 Que será complementada por toda a legislação que está em discussão perante os órgãos legislativos europeus.

reito penal. Alterando diversas leis, incluiu a Lei 83/2017, de 18 de agosto, que estabelece medidas de natureza preventiva e repressiva de combate ao branqueamento de capitais e ao financiamento do terrorismo (BC/FT)[223].

Diante dessa alteração, o Banco de Portugal passa a ser a autoridade competente e responsável quer pelo registro das entidades que exerçam atividades com ativos virtuais, quer pela verificação do cumprimento, por estas entidades, das disposições legais e regulamentares aplicáveis em matéria de prevenção do BC/FT. Todavia, ressalte-se que tal competência se circunscreve apenas à prevenção referida, ou seja, não se alarga a outros domínios, seja de natureza prudencial, comportamental ou outro âmbito[224].

Já a Lei 79/2021 modifica a Lei do Cibercrime (Lei 109/2009) para inserir o art. 3°-G, o qual inclui, para todos os efeitos, sistema ou meio de pagamento aquele que tenha por objeto moeda virtual. Assim, tal modificação também se circunscreve ao âmbito criminal.

Em relação à tributação, até então apenas existia entendimento da Autoridade Tributária e Aduaneira (AT), através da Informação Vinculativa constante do Processo nº 5717/2015, por despacho de 27.12.2016, que estabelecia que só seriam tributados em sede de IRS os lucros com a compra e venda de moeda virtual em Portugal caso se esteja, pela habitualidade, diante de atividade profissional ou empresarial. Neste caso, a tributação ocorreria pela categoria B, sendo descartadas as possibilidades de tributação pelas categorias G e E[225], ainda que obrigado a cumprir as obrigações declarativas constantes do nº 6 do art. 3º do Código do IRS, ou seja, a emitir fatura ou documento equivalente (fatura-recibo eletrônico) sempre que realizar uma venda ou prestar um serviço.

Todavia, aprovou-se recentemente regime fiscal aplicável aos criptoativos através da Lei do Orçamento do Estado de 2023. Neste ficou definida a tributação da pessoa singular nas categorias G (ocorre na mais-valia na

---

223 Informações constantes em: <URL:https://www.bportugal.pt/comunicado/banco-de-portugal-passa-supervisionar-ativos-virtuais-na-prevencao-de-branqueamento-de>, consult. 23.02.2022. As referidas atividades com ativos virtuais são (i) serviços de troca entre ativos virtuais e moedas fiduciárias ou entre um ou mais ativos virtuais; (ii) serviços de transferência de ativos virtuais; e (iii) serviços de guarda ou guarda e administração de ativos virtuais ou de instrumentos que permitam controlar, deter, armazenar ou transferir esses ativos, incluindo chaves criptográficas privadas.

224 Conforme resta informado em: <URL:https://www.bportugal.pt/page/moedas-virtuais?mlid=2808> e <URL:https://www.bportugal.pt/page/registo-de-entidades-que-exercem-atividades-com-ativos-virtuais>, consult. 23.02.2022.

225 Para mais informações, indica-se Liliana Pereira e Juliana Ferreira, "A Tributação do Rendimento Derivado das Transações com a Moeda Virtual "Bitcoin", *In LegalTech, Artificial Intelligence and the Future of Legal Practice*, Veiga, Fábio da Silva; Zalucki, Mariusz (coords.), Porto/Kraków, Instituto Iberoamericano de Estudos Jurídicos and AFM Kraków University, 2022, pp. 327-328. Processo Disponível em <URL:https://info.portaldasfinancas.gov.pt/pt/informacao_fiscal/informacoes_vinculativas/rendimento/cirs/Documents/PIV_09541.pdf>, consult. 23.02.2022.

alienação), B (ocorre na emissão ou mineração de criptoativos, no recebimento de direito de autor no caso de proprietário originário NFT's e ainda pelo princípio do efeito de atração de rendimentos de outras categorias) e E (aplicação residual, para tributar qualquer forma de remuneração decorrente de operações relativas a criptoativos). Também restou prevista a tributação da pessoa coletiva com IRC no caso de variações patrimoniais positivas.

Já em relação ao IVA[226], imposto que tem regras gerais definidas em âmbito comunitário, a AT tratou também por Informação Vinculativa o Processo n° 14763, pelo despacho de 28.01.2019. Neste caso, conforme jurisprudência do Tribunal de Justiça da União Europeia[227], restou considerada prestação de serviços a atividade de câmbio de criptomoedas (no caso o *bitcoin*) por divisas tradicionais e vice-versa, efetuada mediante contraprestação. Porém, concluiu-se que, caso tributável em território nacional, em resultado da aplicação das regras de localização previstas no nº 6 e seguintes do artigo 6º, o prestador de serviços deve aplicar a isenção prevista no artigo 9º, nº 1, alínea 27, subalínea d), do CIVA, muito embora fique obrigado a emitir a correspondente fatura[228].

Diante do vácuo legislativo quanto ao enquadramento jurídico e, até recentemente, fiscal dos criptoativos, restou à doutrina[229] tentar interpretar e lançar luzes sobre a natureza destes ativos para tentar enquadrá-los no ordenamento já existente.

Destaque-se, pela profundidade da abordagem e por enfrentar a temática não somente dos *payment tokens*, mas também dos *utility* e *security tokens*, a doutrina de Maia[230] acerca da tributação nos atos de compra e venda de criptoativos em sede de IRS. Nesta seara, propõe incidência da categoria B se o sujeito passivo realizar compra e venda de criptoativo com caráter de habitualidade e intenção da revenda no momento da compra; e incidência da

---

226 Registre-se que as propostas atualmente em discussão em âmbito europeu não veiculam tributação sobre IVA.

227 Acórdão do TJUE em processo envolvendo Administração Fiscal da Suécia e David Hedqvist (Processo C-264/14) entendeu que as operações de câmbio de criptomoedas em moedas fiduciárias e vice-versa não estavam sujeitas a IVA por se tratar de trocas de diferentes meios de pagamento.

228 Para mais informações, indica-se Joana Alexandre Giraldes Vieira Luz, *Op. Cit*., pp. 20-21, e José Engrácia Antunes (2021a), *Op. Cit*., pp. 10-11. Processo Disponível em <URL:https://info.portaldasfinancas.gov.pt/pt/informacao_fiscal/informacoes_vinculativas/despesa/civa/Documents/INFORMACAO_14763.pdf>, consult. 23.02.2022.

229 Por exemplo, conforme conclusões de Sara Campelo Rocha Areia de Carvalho, *Bitcoin: Do Enquadramento Jurídico à Tributação*, Dissertação (Mestrado em Direito), Universidade Católica Portuguesa, Porto, 2018, p. 54, seguida por Liliana Pereira e Juliana Ferreira, *Op. Cit*., pp. 330-331, entende-se que as criptomoedas deveriam ser regulamentadas como valores mobiliários, dentro do conceito de ativos financeiros, sendo tributadas as suas trocas (por moeda tradicional ou por bens e serviços) pelo regime das mais-valias da categoria G do IRS. Também diferencia da atividade de mineração, que não deveria ser tributada quando da obtenção de criptomoedas como retorno do trabalho desenvolvido.

230 Guilherme Campos Maia, *Op. Cit*., pp. 29-46.

categoria E para os frutos gerados por *security tokens* (incluídos os lastreados em ativos), desde que não prejudique a substância da fonte nem seja passível de ser tributado noutras categorias. Todavia, sobre a incidência da categoria G, conclui não haver resposta suficientemente clara e assertiva quanto à adequada subsunção ao enquadramento dos criptoativos como instrumentos financeiros, o que gera incerteza jurídica e desrespeito aos princípios da igualdade, proporcionalidade e capacidade contributiva diante da lacuna legislativa quanto à regulação do mercado de criptoativos.

Ainda em sede de IRS, merece destaque observação feita por Teixeira[231] (S. d., p. 50) ao opinar que devem ser abrangidos e tributados os pagamentos de criptomoedas a título de mais-valias, rendimentos de capitais ou trabalho dependente, o que não ocorre no ordenamento jurídico português, que tributa apenas rendimentos empresariais e comerciais.

Também há que se salientar o trabalho de Teixeira[232] acerca da tributação das criptomoedas, em especial o *bitcoin*, em sede de IVA. Afora o caso específico Hedqvist, em que se considerou isentas de câmbio as trocas de unidades de moedas virtuais por moedas com curso legal, estabeleceu que quando há incidência de IVA em transferências onerosas de bens digitais, será fixada enquanto prestação de serviços. Assim, conclui ser importante a criação de um quadro regulatório completo que abrangesse todo esse ecossistema criado pelas criptomoedas, objetivando combater riscos de fraude e evasão fiscais e garantir a correta cobrança do imposto no âmbito das prestações de serviços por via eletrônica com contraprestação em moedas virtuais (pp. 50-53)[233].

Em relação ao Brasil, apenas recentemente foi aprovada legislação específica sobre o tema, qual seja, Lei 14.478/2022. Até então apenas existiam manifestações do Banco Central do Brasil (Comunicados 25.306/2014

---

231 Glória Teixeira, "Reforma do Sistema Fiscal – IRS", *In Uma Reforma Fiscal para o Século XXI* [Em linha], AA. VV., Partido Social Democrata, [S. l], [S. d.], pp. 45-54, disponível em <URL:https://www.psd.pt/pt/cen/reforma-fiscal-para-o-seculo-xxi>, consult. 18.07.2022, p. 50.

232 Vanessa Jordana da Silva Teixeira, *A tributação em sede de IVA de Moedas Virtuais no âmbito da União Europeia: o caso do Bitcoin*, Dissertação (Mestrado em Direito), Faculdade de Direito da Universidade do Porto, Porto, 2017.

233 Registre-se ainda os recentes trabalhos de Adriana Macedo, *Tributação das criptomoedas: enquadramento fiscal dos rendimentos derivados das criptomoedas em sede de IRS*, Dissertação (Mestrado em Direito), Faculdade de Direito da Universidade do Porto, Porto, 2021, Mariana Pimenta Ferreira de Carvalho, *Criptomoedas: alguns problemas de regime,* Dissertação (Mestrado em Direito), Faculdade de Direito da Universidade do Porto, Porto, 2021, e Manuel Luís Moura Jacob, *A Tributação dos Criptoativos*, Dissertação (Mestrado em Direito), Universidade Católica Portuguesa, Porto, 2022.

e 31.379/2017[234]), da Comissão de Valores Mobiliários (Nota sobre ICO[235] e Ofícios Circulares de n° 1 e 11/2018[236]) e da Receita Federal do Brasil[237], porém sem a necessária padronização e coerência nos entendimentos. Exemplo disto é a compreensão da CVM de que as criptomoedas são ativos não fi-

[234] Por meio dos Comunicados 25.306/2014 (disponível em <URL:https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=114009277>) e 31.379/2017 (disponível em <URL:https://www.legisweb.com.br/legislacao/?id=352560>), o BACEN informa que os criptoativos não são moedas, nem mesmo eletrônicas, de acordo com a Lei n° 12.865/2013, pois não há supervisão nem regulação por autoridade monetária de nenhum país e, portanto, inexiste garantia de conversão para moeda oficial. Delimitam-se riscos de utilização, inclusive a possibilidade de serem veículos de atividades criminosas, nos mesmos moldes já trazidos em território português.

[235] A CVM lançou em 2017 uma Nota sobre *Initial Coin Offering* (ICO). Destaca que, enquanto captação pública de recursos tendo como contrapartida *tokens* ou *coins*, estes ativos virtuais podem representar valores mobiliários nos termos do art. 2º, da Lei 6.385/76, a depender do contexto econômico de sua emissão e dos direitos conferidos aos investidores, estando, neste caso, sujeitos à regulação e legislação específicas. Assim, dentro de sua competência, esclarece que "tais valores mobiliários ofertados por meio de ICO não podem ser legalmente negociados em plataformas específicas de negociação de moedas virtuais, uma vez que estas não estão autorizadas pela CVM a disponibilizar ambientes de negociação de valores mobiliários no território brasileiro". Por fim, elenca diversos riscos em investir nesse segmento, como fraudes, atividades criminosas, volatilidade, liquidez, cibernéticos e operacionais. Disponível em <URL:https://conteudo.cvm.gov.br/noticias/arquivos/2017/20171011-1.html>, consult. 27.02.2022.

[236] O Ofício Circular 1/2018 (Disponível em <URL:https://conteudo.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-0118.html>) basicamente registra que como as criptomoedas não podem ser qualificadas como ativos financeiros (artigo 2º, V, da Instrução CVM nº 555/14), não é permitida sua aquisição direta por fundos de investimentos daí regulados. Já o Ofício Circular 11/2018 (Disponível em <URL:https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/oficios-circulares/sin/anexos/oc-sin-1118.pdf>), em complemento ao anterior, "autoriza o investimento indireto em criptoativos por meio, por exemplo, da aquisição de cotas de fundos e derivativos, entre outros ativos negociados em terceiras jurisdições, desde que admitidos e regulamentados naqueles mercados. No entanto, no cumprimento dos deveres que lhe são impostos pela regulamentação, cabe aos administradores, gestores e auditores independentes observar determinadas diligências na aquisição desses ativos", minimizando os riscos já elencados.

[237] Desde 2017 já havia informação em seu sítio eletrônico, no campo Perguntas e Respostas Imposto de Renda Pessoas Físicas, que as até então "moedas virtuais" estariam sujeitas à tributação pelo ganho de capital, por serem equiparadas a ativos financeiros. Disponível em <URL:https://www.gov.br/receitafederal/pt-br/assuntos/irpf/2020/perguntao/pir-pf-2017-perguntas-e-respostas-versao-1-1-03032017.pdf>. Tal se manteve inalterado até 2021, em face das regras instituídas pela Instrução Normativa RFB nº 1.888/2019, quando se adiciona o termo criptoativos junto a moedas virtuais, passando a diferenciá-los entre *bitcoins*, *altcoins* e os demais criptoativos não considerados criptomoedas. Disponível em <URL:https://www.gov.br/receitafederal/pt-br/acesso-a-informacao/perguntas-frequentes/declaracoes/dirpf/pr-irpf-2021-v-1-0-2021-02-25.pdf>, consult. 27.02.2022.

nanceiros, enquanto que a RFB entende que equivalem a ativos financeiros para fins tributários[238].

Na seara tributária, o único regulamento existente fora elaborado em 03 de maio de 2019, pela RFB, através da Instrução Normativa 1.888, alterada pela Instrução Normativa RFB nº 1.899, de 10 de julho de 2019[239], que institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos para fins tributários. Trata-se de preocupação eminentemente fiscal e arrecadatória.

Conforme o art. 6°, previu-se a obrigatoriedade de prestar informações tanto das *exchanges* de criptoativos[240] domiciliadas no Brasil para fins tributários como das pessoas físicas ou jurídicas residentes ou domiciliadas no Brasil, neste caso quando as operações mensais ultrapassarem R$ 30.000,00 (trinta mil reais) e forem realizadas em *exchange* domiciliada no exterior ou em operações não realizadas por *exchange* (ou seja, entre particulares ou P2P). As operações se relacionam a compra, venda, permuta, doação, retirada, cessão temporária, dação em pagamento, emissão e outras operações que impliquem em transferência. *A contrario sensu*, verifica-se que tais obrigações não estão previstas para *exchanges* ou pessoas que não possuam residência ou domicílio em solo brasileiro.

Dentre as informações a serem prestadas para cada operação, conforme o art. 7°, destacam-se data, tipo, titulares e valor da operação, quantidade e modalidade de criptoativos negociados, e valor das taxas de serviços cobrados para a execução. Com relação aos titulares da operação, devem ainda constar o nome, endereço, domicílio fiscal, número de identificação e demais informações cadastrais[241].

---

238 Outro exemplo é que a Resolução CVM 50, de 31 de agosto de 2021 (que revogou a Instrução CVM 617/2019 e sua Nota Explicativa), que dispõe sobre a prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (PLD/FTP) no âmbito do mercado de valores mobiliários, não sujeita (ao menos não expressamente, ponto digno de nota, diante da necessidade de promover segurança jurídica aos *players*) às suas obrigações as pessoas físicas ou jurídicas que atuam na criptoeconomia com ativos que possam se configurar como valores mobiliários, conforme seu art. 3°.

239 Texto da IN 1.888/2019, com as alterações da IN 1.889/2019, encontra-se Disponível em <URL:http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592>, consult. 27.02.2022.

240 Definida no art. 5°, II, como pessoa jurídica (excluindo-se, portanto, as pessoas físicas do conceito), ainda que não financeira, que oferece serviços referentes a operações realizadas com criptoativos, inclusive intermediação, negociação ou custódia, que pode aceitar quaisquer meios de pagamento, inclusive outros criptoativos.

241 Tendo em vista fugir ao escopo do trabalho, para conhecimento acerca de aparente atecnia quanto ao conceito de criptoativos, bem como do cenário de desproporcionalidade das obrigações acessórias veiculadas pela RFB, exorbitando seus limites e competência, indica-se Dayana de Carvalho Uhdre, *Op. Cit*., pp. 160-171.

Com relação ao aspecto arrecadatório, resta previsto que os criptoativos de uma forma geral são tributados no Brasil a título de ganho de capital, na hipótese de haver ganhos obtidos com a alienação destes bens cujo total no mês superar o importe de R$ 35.000,00 (trinta e cinco mil reais). As alíquotas são progressivas, podendo variar de 15% (quinze por cento) a 22,5% (vinte e dois e meio por cento), e o recolhimento deve ser feito até o último dia do mês seguinte ao da transação.

Por sua vez, importa registrar e louvar os termos da Instrução CVM 626, de 15 de maio de 2020, posteriormente substituída pela Resolução CVM nº 29/21, que dispõe sobre as regras para constituição e funcionamento de ambiente regulatório experimental, intitulado *sandbox* regulatório, em que "as pessoas jurídicas participantes poderão receber autorizações temporárias para testar modelos de negócio inovadores em atividades no mercado de valores mobiliários regulamentadas pela Comissão de Valores Mobiliários". Entre as finalidades, destacam-se o fomento à inovação no mercado de capitais, diminuição de custos e de tempo de maturação para desenvolver produtos, serviços e modelos de negócios inovadores[242]. Proporciona-se, desse modo, ambiente regulatório experimental, potencializando o empreendedorismo no setor.

Ressalte-se ainda o recente Parecer de Orientação CVM nº 40[243], que consolida o seu entendimento sobre as normas aplicáveis aos criptoativos que forem valores mobiliários, esclarecendo os limites de atuação e a forma como pode e deve exercer seus poderes para normatizar, fiscalizar e disciplinar a atuação dos integrantes do mercado de capitais. Com inspiração americana no *Howey Test* e prezando pela transparência do mercado, entende que podem ser considerados valores mobiliários os criptoativos que sejam representação digital de algum dos valores mobiliários previstos taxativamente nos incisos I a VIII do art. 2º da Lei nº 6.385/76 e/ou previstos na Lei nº 14.430/2022, bem como na possibilidade de enquadramento no conceito aberto de valor mobiliário do inciso IX do art. 2º da Lei nº 6.385/76, na medida em que seja contrato de investimento coletivo.

Por fim, destaca-se que recentemente fora aprovada a Lei 14.478/2022, objetivando pretensa regulação do setor. Para isto, dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais. Muito embora

---

242 Previu-se o Comitê de Sandbox, criado pela Portaria CVM/PTE 75/20 (Disponível em <URL:https://conteudo.cvm.gov.br/menu/acesso_informacao/institucional/comites/comite_sandbox.html>) e responsável pela condução de atividades específicas relacionadas. Registra-se que a CVM já finalizou o primeiro processo de admissão do *sandbox* regulatório, conforme se verifica em: <URL:https://www.gov.br/cvm/pt-br/assuntos/noticias/cvm-finaliza-primeiro-processo-de-admissao-do-sandbox-regulatorio#:~:text=As%20datas%20de%20in%C3%ADcio%20das,de%20prepara%C3%A7%C3%A3o%20operacional%20e%20comercial>, consult. 27.02.2022.

243 Disponível em <URL:https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html>, consult. 15.04.2023.

se verifique que padece de omissões quanto à complexidade do ambiente de negócios que se presta a regular[244] e que dá ao Poder Executivo a incumbência de atuar como legislador em algumas matérias[245], identificam-se avanços para proporcionar a necessária segurança jurídica ao ambiente empresarial que desenvolve suas atividades no setor, com potencial de ganhos na atração de investimentos ao território nacional e competitividade em relação ao cenário internacional[246]. Porém, fora retirada da legislação previsão importante e que, por isso, merece crítica: a manutenção segregada de recursos aportados pelos clientes dos recursos da prestadora de serviços.

Dito isto, não havendo regulação específica até então, coube ao intérprete jurídico, entre doutrina e jurisprudência, buscar identificar os fins de cada criptoativo para, em seguida, direcionar o regime jurídico já existente e aplicável ao caso concreto. Sobremaneira no Brasil, federação composta pela União, Estados, Municípios e Distrito Federal, cada qual com suas competências e materialidades para tributar, limitadas pela Constituição Federal e por lei complementar, mas que recorrentemente geram controvérsias a serem resolvidas pelos intérpretes do Direito, o que se potencializa em cenário econômico ainda não regulado.

Sob o aspecto criminal, o Superior Tribunal de Justiça já decidira que as moedas virtuais não são tidas pelo BACEN como moeda nem pela CVM como valor mobiliário, não caracterizando sua negociação, por si só, nos

---

244 Não se visualiza, por exemplo, normas específicas acerca dos NFTs, *tokenização* de ativos virtuais e reais, e das *stablecoins* enquanto importante interface a ser delineada entre criptomoedas e as chamadas *Central Bank Digital Currencies* (CBDCs). Verifica-se que o projeto do Real Digital poderá iniciar sua fase de lançamento já em 2024.

245 Como se verifica quanto ao procedimento simplificado de autorização para funcionamento das prestadoras de serviços de ativos virtuais; quanto à definição dos ativos financeiros regulados para os fins desta lei; e quanto à definição do órgão ou entidade responsável pela disciplina do funcionamento, da supervisão e do cancelamento da autorização dessas prestadoras.

246 Destacam-se as seguintes matérias: (1) inaplicabilidade desta lei aos ativos representativos de valores mobiliários, que ficam sujeitos ao regime da Lei nº 6.385, de 7 de dezembro de 1976, e não altera nenhuma competência da Comissão de Valores Mobiliários; (2) não inclusão no conceito de ativo virtual a moeda nacional e estrangeiras, a moeda eletrônica, os *tokens* de utilidade e as representações de ativos previstos em lei ou regulamento; (3) autorização prévia para que as prestadoras de serviços possam funcionar no país; (4) estabelecimento de diretrizes gerais de atuação no mercado, como boas práticas de governança, transparência nas operações e abordagem baseada em riscos, segurança da informação e proteção de dados pessoais, proteção e defesa dos consumidores, usuários e da poupança popular, bem como prevenção à lavagem de dinheiro; (5) inclusão no Código Penal do art. 171-A, estabelecendo fraude em prestação de serviços de ativos virtuais, valores mobiliários ou ativos financeiros, em alusão aos crimes piramidais; (6) equiparação da pessoa jurídica prestadora de serviços com ativos virtuais à instituição financeira para fins da legislação penal acerca do sistema financeiro nacional (Lei 7.492/86); (7) inserção expressa das prestadoras de serviços de ativos virtuais na condição de sujeito de obrigações da nossa lei antilavagem de dinheiro (Lei 9.613/98), e (8) aplicação expressa das disposições do Código de Defesa do Consumidor.

crimes tipificados nos artigos 7º, II, e 11, ambos da Lei 7.492/1986 (define os crimes contra o sistema financeiro nacional), nem mesmo no delito previsto no art. 27-E, da Lei 6.385/1976 (crime contra o mercado de capitais). Na mesma decisão, destaca-se restar possível o cometimento do delito do *caput* do art. 22, da Lei 7.492/86 (evasão de divisas na forma própria, por meio de exportação não autorizada, dentro do sistema) quando a aquisição for utilizada para fins de efetivação de contrato de câmbio ilegal, cujo objetivo seja a evasão de divisas em desconformidade às regras do BACEN[247].

Por outro lado, recentemente o STJ decidiu por diferenciar a situação em que os criptoativos sejam distribuídos de forma a caracterizar oferta pública e captação de investimento público, incidindo as disposições da Lei 7.492/1986. Neste caso, poderão ser considerados valores mobiliários na forma do art. 2°, IX, cumulado com art. 19, §3º, da Lei 6.385/79 (oferta de contratos de investimentos coletivos), bem como meio para a prática de crimes contra o sistema financeiro nacional, nomeadamente dos artigos 4º, 5º, 7º, 11 e 16[248].

Por fim, destaque-se a visão de Nunes[249], ao concluir que "ainda que não regulamentada pelo BACEN e/ou CVM a utilização não autorizada do *bitcoin* como meio para realização de operação de câmbio, poderá configurar, em tese, os delitos de evasão de divisas" previstos também nas "modalidades de evasão-envio (utilização da técnica do 'bitcoin-cabo') e evasão depósito (manutenção de divisas em contas no exterior não declaradas ao BACEN, quando oriundas da utilização da negociação de *bitcoin* como meio para aquisição de moeda estrangeira)", conforme parágrafo único do art. 22 da Lei 7.492/86.

Sob a perspectiva tributária, a doutrina se concentrou na análise das criptomoedas. Em consonância com o regramento da RFB, o entendimento de Steffens e Tessari[250] é pela incidência de imposto de renda sobre o ganho de capital obtido com a alienação de criptomoedas, com a aquisição destas através de moeda de curso forçado e ainda com a aquisição de mercadorias utilizando criptomoedas (neste caso a criptomoeda será utilizada com meio de pagamento e a operação caracterizada como permuta). Neste último caso, poderá a operação dar ensejo à cobrança de ICMS, no caso de aquisição de mercadoria, ISS, no caso de pagamento pela prestação de serviço, ou de ITBI, na hipótese de aquisição de imóvel. Por fim, a referida doutrina ainda destaca incidência de ITCMD para o caso de doação de criptomoedas

247 STJ. CC 161.123/SP, Rel. Ministro SEBASTIÃO REIS JÚNIOR, TERCEIRA SEÇÃO, julgado em 28.11.2018, DJe 05.12.2018. Disponível em <URL:https://scon.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=CC+161123&b=ACOR&p=false&l=10&i=5&operador=E&tipo_visualizacao=RESUMO>, consult. 28.02.2022.

248 STJ. HC 530.563/RS, Rel. Ministro SEBASTIÃO REIS JÚNIOR, SEXTA TURMA, julgado em 05.03.2020, DJe 12.03.2020. Disponível em <URL:https://scon.stj.jus.br/SCON/pesquisar.jsp?newsession=yes&tipo_visualizacao=RESUMO&b=ACOR&livre=HC+530563>, consult. 28.02.2022.

249 Leandro Bastos Nunes, *Op. Cit*..

250 Luana Steffens e Cláudio Tessari, *Op. Cit*., pp. 6-7.

ou transmissão pela ocorrência da morte do seu titular. Piscitelli[251] destaca ainda a incidência de tributação na permuta de criptomoedas, diante da aparente realização, mensurável economicamente.

Em Uhdre[252], igualmente sobre criptomoedas, destacam-se alguns entendimentos: (i) equiparação de *trade* e *day-trade* ao regime jurídico-tributário do mercado de ações; (ii) tributação de pessoas jurídicas pelo ganho ou perda enquanto ativo não operacional (exceto nos casos de *exchanges*, que serão tratados como operacionais)[253], correspondente à diferença positiva entre o valor da alienação e contábil (ou seja, o valor originalmente transacionado); (iii) não incidência de IOF-Câmbio para criptomoedas por não se poder considerá-los como moeda estrangeira; (iv) *exchanges* de criptomoedas tributadas por ICMS-Mercadoria no caso de adquiri-las para estoque e vendê-las em suas plataformas, ou, regra geral, por ISS no caso de prestadoras de serviços e intermediadores dos negócios[254]; (v) mineradores tributados por ISS apenas pelos serviços prestados e remunerados pelas taxas cobradas diretamente dos usuários para validação de suas operações, mas isentos no caso de recebimento de recompensas pela criação de novos blocos na *blockchain*, diante da inocorrência de bilateralidade entre prestador e tomador do serviço[255].

Por fim, diante da originalidade da abordagem, tem-se destaque a doutrina de Gomes[256]. Além de opinar acerca do não cabimento de ICMS e IOF e

---

251 Tathiane Piscitelli, *Op. Cit*., p. 16.

252 Dayana de Carvalho Uhdre, *Op. Cit*., pp. 215-235.

253 Thiago Rufalco Medaglia e Eric Simões Visini, *Op. Cit*., p. 635, tratando sobre criptomoedas, diferenciam entre empresas que têm como objeto social o comércio de ativos financeiros, que deverão tratar as receitas decorrentes da negociação desses ativos como operacionais (venda de ativo circulante), e empresas que tratem esse tipo de ativo como investimento financeiro de longo prazo, tratando tal operação como venda de ativo não circulante, tributando o ganho de capital eventualmente registrado. Inclusive, destacam não haver diferença de enquadramento na prática de arbitragem de criptoativos enquanto "processo de compra e venda dessas moedas de forma simultânea, em diferentes mercados, de sorte a auferir lucro com a combinação de operações", aplicando-se o mesmo regime da compra e venda, bem como incidindo ISS para empresas que cobram taxas pela prestação de tal serviço (*Op. Cit*., p. 639).

254 Destaque-se a opinião contrária de Luana Steffens e Cláudio Tessari, *Op. Cit*., p. 7 sobre a incidência de ISS, tendo em vista a ausência da previsão expressa da atividade da *exchange* na lista anexa à Lei Complementar 116/03, em atenção ao princípio da tipicidade e legalidade tributária e a taxatividade definida pelo STF no Tema 296.

255 Segundo Barbara das Neves e Pedro Vitor Botan Cíceri, *Op. Cit*., p. 28, e Tathiane Piscitelli, *Op. Cit*., p. 11, existiria fato sujeito à incidência do Imposto de Renda quando da saída ou realização desses criptoativos em relação ao ganho de capital.

256 Daniel de Paiva Gomes, *Bitcoin: a tributação de investimentos em criptomoedas*, Dissertação (Mestrado em Direito), Fundação Getúlio Vargas, São Paulo, 2019, pp. 266-275. Trabalho de dissertação atualizado para importante obra: Daniel de Paiva Gomes, *Bitcoin: a tributação de criptomoedas: da taxonomia camaleônica à tributação de criptoativos sem emissor identificado*, São Paulo, Revista dos Tribunais, Thomson Reuters Brasil, 2021.

da não equiparação das criptomoedas em ativos financeiros, de forma contrária ao entendimento da RFB, evidencia a utilização de uma abordagem funcional em detrimento da busca por uma qualificação jurídica estanque das criptomoedas, enquanto ativos camaleônicos com funções de meio de pagamento ou de investimento especulativo. Assim, tomando por base que a qualificação jurídico-tributária das criptomoedas no cenário internacional toma como hipóteses de incidência a consideração destes ativos enquanto propriedade, ativos financeiros e moeda estrangeira, conclui ser a finalidade que deveria definir a tributação, como já ocorre com o ouro, tributado, de acordo com a sua destinação, pelo IOF ou ICMS.

Verifica-se, em resumo, insegurança jurídica com a multiplicidade de soluções trazidas pela doutrina e, de forma incipiente e fragmentária, formalmente integradas pelos ordenamentos jurídicos nacionais que regularam a matéria. Assim, conforme se vislumbra Antunes[257], são postos diferentes aspectos multidisciplinares neste contexto a gerarem discussões variadas quanto à aplicação da correta disposição legal ao caso concreto, destacando-se os planos obrigacional, real, fiscal, internacional privado e penal[258]. Portanto, são frequentes entendimentos divergentes e contraditórios entre si, o que dificulta sobremaneira a conformidade dos diversos *players* em ambiente de negócios internacional.

5. PERSPECTIVA REGULATÓRIA INTERNACIONAL

No capítulo anterior, ao se verificarem iniciativas regulatórias no ambiente soberano de alguns dos mais relevantes países no cenário dos criptoativos, verifica-se de pronto a existência de diferenças flagrantes de entendimentos. Seja pela classificação dos tipos de *tokens*, o que releva para efeito de natureza jurídica e, consequentemente, da legislação tributária aplicada a cada manifestação de riqueza. Seja pelos requisitos de licença para atuar no mercado ou de garantias aos investidores que se interessem em utilizar os serviços oferecidos, seja ainda pelas obrigações a que estão vinculados os diversos *players* para prevenir ou eventualmente reprimir o cometimento de ilícitos.

Com isto, importa neste capítulo verificar a existência de indicativos regulatórios em ambiente internacional, que podem servir de baliza para o entendimento de cada Estado soberano, mesmo que sem vinculação direta, efetiva e automática. Desta forma, vislumbrando-se que a evolução legislativa de cada país não consegue acompanhar tempestivamente o desenvolvimento tecnológico pujante e ininterrupto dos criptoativos, possibilita-se atingir de

[257] José Engrácia Antunes (2021a), *Op. Cit*., pp. 32-35.

[258] Isto sem falar em projeções do direito societário, mercado de capitais, contabilístico, insolvência, consumo, processual e até sucessões. Para mais detalhes, v. José Engrácia Antunes (2021b), *Op. Cit*., pp. 252-260.

forma madura a apreensão da proposta que se ventila no último capítulo deste trabalho, ainda que limitada diante dos limites deste trabalho e a complexidade, atualidade e efemeridade do tema, em constante mutação.

Por isso, ainda que de extrema importância o enfrentamento de aspectos como a taxonomia (considerada em suas esferas de catalogação e classificação) correta dos tipos de *tokens* ou criptoativos, pois tal impacta no entendimento sobre a respectiva natureza e qualificação jurídica, inclusive vinculando o legislador acerca do fato gerador para fins tributários (sejam com o fim de declaração, arrecadação ou fiscalização), optou-se pela divisão entre *payment tokens*, *security tokens* e *utility tokens*. Sem prejuízo da necessidade de proceder à proposta de sistematização, o que será feito em trabalho vindouro[259].

De toda sorte, destaque-se nesta seara a iniciativa da *International Organization for Standartization*, numerada como ISO 22739:2020 e intitulada como "*Blockchain and distributed ledger technologies — Vocabulary*"[260], que objetiva proporcionar padronização semântica aos diversos termos utilizados neste universo. Todavia, em que pese louvável, além de não possuir vinculação jurídica, é somente adquirida por prestação pecuniária, o que dificulta a disseminação do conhecimento proporcionado.

5.1. DA CONVENÇÃO DE BUDAPESTE ÀS RECOMENDAÇÕES DO GAFI

Retomando a análise feita no segundo capítulo acerca da cibercriminalidade, desde o início da década de 2000 o tema causa preocupação na comunidade internacional. Como exemplos, a reunião de ministros da justiça e procuradores dos países integrantes da Organização dos Estados Americanos (OEA) em março de 2000, cujo tema foi o combate de ações de *hackers* na internet[261], e o Fórum Mundial de Governança na Internet de 2007, apoiado pela ONU e sediado no Rio de Janeiro, em que se concluiu que

---

259 Ressalte-se, por enquanto, análise minuciosa empreendida por Dayana de Carvalho Uhdre, *Op. Cit*., pp. 57-97. Elenca tanto propostas a título doutrinário, como a de Don Tapscott e Alex Tapscott, que divide os criptoativos em 7 categorias; como de órgãos oficiais, como o FMI e a OCDE. Passa pela catalogação em 5 dimensões (propósito, utilidade, status legal, valor subjacente e camada técnica) feita por Thomas Euler em conjunto com bolsistas do Untitled INC, importante por se propor como aberta e atualizável de acordo com a verificação de inovações no setor; bem como pela diferenciação entre ativo nato da própria rede distribuída ou de ativo existente no mundo físico feito pela *Token Alliance*, da *Chamber of Digital Commerce*. Por fim, apresenta proposta doutrinária própria, em exercício de classificação em dois passos: primeiramente estabelecendo ser um ativo tokenizado ou nativo da DLT e, em seguida, dividindo-se o *token* entre *currency*, *utility* ou *security*.

260 Disponível em <URL:https://www.iso.org/standard/73771.html>, consult. 03.04.2022.

261 Informado por Reginaldo César Pinheiro, *Os cybercrimes na esfera jurídica brasileira* [Em linha], 2000, disponível em <URL:http://jus.com.br/revista/texto/1830>, consult. 10.06.2020.

"nenhuma ação de combate a crimes virtuais ou a ameaças que circulam na internet seja efetiva sem que haja uma cooperação internacional"[262].

Assim, afora a atuação individual de países como Estados Unidos, Inglaterra e Índia[263], considerando a necessidade de combate mundial ao fenômeno, em 2001 o Conselho da Europa, através do Comitê Europeu para os Problemas Criminais, cria a Convenção de Budapeste sobre o Cibercrime[264], que entra em vigor em 2004 com a ratificação de cinco países. Enquanto primeiro tratado acerca do tema, são 66 (sessenta e seis) países que já ratificaram e aderiram[265], porém outros 158 (cento e cinquenta e oito) utilizaram seus termos como orientação para elaborar suas legislações nacionais de combate aos crimes cibernéticos.

Através do documento, resta estabelecida política criminal comum, indicando a adoção de medidas a serem tomadas a nível nacional por cada membro, tanto em direito penal material, ao tipificar condutas, como em direito processual, com medidas de persecução penal e de competência de atuação. Também são indicados princípios gerais de cooperação internacional, procedimentos de auxílio mútuo e a previsão de existência de uma rede ininterrupta (intitulada "24/7") para prestação de assistência imediata a investigações ou procedimentos respeitantes a infrações penais relacionadas com dados e sistemas informáticos, ou ainda a fim de recolher provas, sob forma eletrônica, de uma infração penal.

Verifica-se a existência de dois protocolos adicionais à convenção. O primeiro, relativo à criminalização de atos de natureza racista e xenófoba praticados através de sistemas informáticos[266], e outro, relativo ao reforço

---

262 Disponível em <URL:https://extra.globo.com/noticias/saude-e-ciencia/internet-mais-segura-depende-de-cooperacao-internacional-defendem-especialistas-651784.html>, consult. 05.04.2022.

263 Conforme se verifica em Tarcísio Teixeira, *Op. Cit*., p. 226, enquanto a Índia implementou em outubro de 2000 a (considerada) primeira lei nacional contra crimes cibernéticos, o "IT Act"; os EUA, por meio do FBI, criaram no mesmo ano o "Centro de Fraude de internet" e ainda um centro de segurança cibernética; e a Inglaterra lançou em 2011 uma Unidade Nacional para Crimes de Alta Tecnologia, com verba de US$ 35 milhões e 40 funcionários de alto escalão, baseados em local secreto, para enfrentar as fraudes, extorsões e lavagem de dinheiro.

264 Texto integral Disponível em <URL:https://rm.coe.int/16802fa428>, consult. 05.04.2022.

265 Lista completa Disponível em <URL:https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>, consult. 05.04.2022.

266 Texto integral em português e aprovado Disponível em <URL:https://files.dre.pt/1s/2009/09/17900/0641506421.pdf>, consult. 05.04.2022.

da cooperação e da comunicação de provas eletrônicas já existentes[267], pendente de abertura para assinatura por parte dos membros[268].

O Brasil, finalmente, aderiu formalmente à convenção com a publicação do Decreto Legislativo 37, de 16 de dezembro de 2021. Assim, diante da pandemia ocasionada pela disseminação da Covid-19, que potencializou a ocorrência de delitos em meio cibernético, somando-se à emergência da Lei 12.965/2014 (Marco Civil da Internet) e mais recentemente da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), será necessário que o legislador federal rediscuta, harmonize e otimize o Direito Penal e Processual Penal brasileiro com foco no cenário internacional. Trata-se de importante passo na uniformização de procedimentos nacionais, bem como cooperação com especialistas em meio global[269].

Por sua vez, o GAFI, dentro de sua atuação institucional, já havia publicado relatórios nos anos de 2014[270] e 2015[271] alertando para os riscos de cometimento do delito de lavagem de dinheiro através de criptomoedas, ainda que reconhecesse os benefícios econômicos atingidos com a inclusão de indivíduos sem acesso ao sistema bancário, a redução de custos e facilitação de transações. Desde então já se alertava sobre a necessidade de estabelecer padrões para a regulação da matéria, através de práticas similares pelas jurisdições nacionais, conforme indicado no segundo documento, que procura adequar as suas 40 recomendações às transações com criptomoedas[272]. É indicado pelo GAFI o foco nas plataformas de negociação (*exchanges*), que têm como função a conversão de criptomoedas em moedas fiduciárias, desencorajando os reguladores a simplesmente proibir transações dessa natureza diante da possível continuidade dos atos ilícitos, desta feita sem controle ou supervisão.

---

267 Texto aprovado e em português Disponível em <URL: https://data.consilium.europa.eu/doc/document/ST-14898-2021-INIT/pt/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Acesso+a+provas+eletr%c3%b3nicas%3a+Conselho+autoriza+Estados-Membros+a+assinarem+um+acordo+internacional>, consult. 05.04.2022.

268 O Conselho da União Europeia adotou decisão na qual autoriza os Estados-Membros a assinarem, no interesse da UE, este segundo protocolo adicional. Disponível em <URL:https://tek.sapo.pt/noticias/computadores/artigos/convencao-do-cibercrime-conselho-da-ue-promove-adesao-a-acordo-que-facilita-acesso-a-provas-eletronicas>, consult. 05.04.2022.

269 Para mais informações, indica-se as análises disponíveis na Internet: <URL:https://itforum.com.br/noticias/brasil-assina-convencao-de-budapeste-e-caminha-para-ciberseguranca-mais-robusta/> e <URL:https://www.migalhas.com.br/depeso/357721/adesao-a-convencao-de-budapeste-sobre-o-crime-cibernetico-e-desafios>, consult. 05.04.2022.

270 Intitulado "*FATF REPORT. Virtual Currencies. Key Definitions and Potential AML/CFT Risks*". Disponível em <URL:https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, consult. 05.04.2022.

271 Intitulado "*Guidance for a Risk-Based Approach. Virtual Currencies*". Disponível em <URL:https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>, consult. 05.04.2022.

272 Para mais informações, Christiana Mariani da Silva Telles, *Op. Cit*., pp. 100-102.

Para tanto, já em 2018, ao dispor sobre Abordagem Baseada em Risco[273], fez novas adequações às suas recomendações, sobremaneira a de n° 15, que trata sobre novas tecnologias. Dispõe que, para gerenciar e mitigar os riscos emergentes dos ativos virtuais, os países devem garantir que provedores de serviços de ativos virtuais sejam regulamentados para fins de AML/CFT e licenciados ou registrados, bem como sujeitos a sistemas eficazes para monitorar e garantir o cumprimento das medidas exigidas nas suas recomendações.

Também fez adições ao seu Glossário, ao incluir definições para "ativos virtuais" e "provedores de serviços de ativos virtuais". Para a primeira definição se excluiu representações digitais de moedas fiduciárias, valores mobiliários e outros ativos financeiros já cobertos em outras recomendações. A segunda são as *exchanges*, certos tipos de provedores de carteira e os provedores de serviços financeiros para Ofertas Iniciais de Moedas (ICOs)[274].

Por sua vez, em 2019 o GAFI publicou um guia de análise de risco de lavagem de capitais e financiamento do terrorismo para o setor das criptomoedas[275]. Objetivando coibir o anonimato, teve como principal recomendação a recolha de informações por parte dos provedores de serviços de ativos virtuais sobre seus clientes, sobremaneira quando da realização de transferências, a exemplo do nome do remetente e do beneficiário, número da conta (*wallet*) e endereço geográfico. Obviamente, o intuito seria de registro dos negócios e comunicação de operações suspeitas.

Por fim, em outubro de 2021 esse guia recebeu atualização importante[276], inclusive com introdução de práticas do sistema bancário ao mercado dos criptoativos, incluindo compliance. Destacam-se o fornecimento de orientações adicionais sobre a chamada "regra de viagem"[277] e ainda a identifica-

---

273 Informações gerais disponíveis na Internet: <URL:http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html>, consult. 05.04.2022.

274 As 40 Recomendações, acompanhadas de notas interpretativas e do Glossário, sofreram nova atualização, datada de março de 2022, Disponível em <URL:http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>, consult. 05.04.2022.

275 Intitulado "*Guidance for a Risk-Based Approach. Virtual Assets And Virtual Asset Service Providers*". Disponível em <URL:https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>, consult. 05.04.2022.

276 Texto integral Disponível em <URL:https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>. Bem como de arquivo sumarizado de seus principais aspectos: <URL: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Quick-guide-RBA-VA-VASPS.pdf>, consult. 05.04.2022.

277 Além do provedor compartilhar dados de clientes com outros provedores, deve também realizar a devida diligência sobre outros provedores com os quais seus clientes realizam transações, na primeira transação identificada com tal provedor. Para tanto, deverá verificar se o provedor atende as normas de regulamentação, bem como se possui estrutura adequada no combate à lavagem de dinheiro e financiamento ao terrorismo, como verificações de KYC e política antilavagem.

ção da contraparte do cliente e imposição de coleta significativa de dados[278]. Também chama atenção a abordagem acerca das transações P2P e dos usuários de carteiras não hospedadas (*cold wallets*), ao sugerir medidas a serem adotadas pelos reguladores para mitigar os riscos nesta seara.

Ainda há que se salientar que os reguladores são aconselhados a adotar uma abordagem expansiva para as definições, atendo-se mais ao ativo ou serviço do que à nomenclatura ou terminologia usada. Isso inclui orientações atualizadas sobre como *stablecoins*, tokens não fungíveis (NFTs), finanças descentralizadas (DeFi) e aplicativos descentralizados ou distribuídos (DApps) estão relacionados aos padrões do GAFI, aplicando-se, dependendo do caso, a regulação destinada aos ativos virtuais e aos provedores de serviços de ativos virtuais, ainda que assim não sejam considerados.

5.2. ENTENDIMENTO DA OCDE EM MATÉRIA TRIBUTÁRIA

A OCDE, organização econômica intergovernamental que conta atualmente com 38 (trinta e oito) países membros (o Brasil ainda não é membro), também em sua esfera de atuação, privilegia o ambiente colaborativo entre as jurisdições para identificação das bases tributáveis cabíveis a cada caso concreto, ao mesmo tempo em que se promovem ganhos em termos de eficiência e redução de custos. O intitulado *Common Reporting Standard* (CRS), aprovado em 2014, já previa um padrão para a obtenção de informações das jurisdições em relação às suas instituições financeiras e a troca automática dessas informações com outras jurisdições[279]. Tudo em combate à evasão fiscal.

Por outro lado, há entendimento plasmado da OCDE desde o ano de 2019 sobre a efetividade da tributação das plataformas na *sharing and gig economy*[280]. Para tanto, formalizou a adoção de medidas para empreender melhor e mais efetiva tributação sobre as plataformas de economia compartilhada, colaborativa e sob encomenda: (i) iniciativas educacionais conjuntas, inclusive em cooperação com as plataformas, para tornar os vendedores mais cientes de suas obrigações fiscais; (ii) padronização dos requisitos de relatórios e informações dos usuários das plataformas, com vistas à sua identificação exata; (iii) cooperação internacional reforçada entre as autori-

---

278 Basicamente são as exigências que o Brasil já previu na Instrução Normativa n° 1.888, no sentido de identificar a origem e destino dos pagamentos que são realizados. Remete-se o leitor para o tópico 5 do capítulo anterior.

279 Mais informações em: <URL:www.oecd.org/tax/automatic-exchange/common-reporting-standard/>, consult. 05.04.2022.

280 S*haring economy* ou economia compartilhada se dá com a utilização de plataformas para oferecimento de serviços e produtos a serem comprados ou alugados em um mercado online, como Uber e Airbnb. G*ig economy* se considera como uma evolução da primeira, podendo ser entendida como "sob encomenda", proporcionando oportunidades de encontro entre trabalhadores *freelancer* e empresas que desejam contratar serviços com taxa de rotatividade rápida e variedade de campos, como Xtras e Managed by Q.

dades fiscais para garantir conformidade com as obrigações disciplinadas nos relatórios; e (iv) troca internacional de informações entre as administrações fiscais sobre vendedores de plataforma residentes em uma jurisdição, mas operando por meio de uma plataforma localizada em outra[281].

O referido relatório disciplina que, embora tenha como escopo ajudar a garantir a tributação efetiva dos vendedores de plataformas de compartilhamento ou sob encomenda, a intenção é que isso não coloque encargos desnecessários sobre os usuários das plataformas, as próprias plataformas e as administrações fiscais. Por isso, adota três recomendações a serem consideradas: (i) diminuição dos encargos de conformidade através da adoção de um modelo de Código de Conduta; (ii) cooperação internacional reforçada com troca contínua de informações sobre práticas bem-sucedidas e abordagens legislativas exitosas para melhorar a compreensão do imposto a ser aplicado; e (iii) desenvolvimento de um modelo legislativo para relatórios padronizados, evitando previsão de requisitos diferentes para as administrações fiscais envolvidas. Tal modelo, inclusive, já foi apresentado pela própria OCDE ainda no ano de 2020, intitulado "*Model Rules for Reporting by Platform Operators with respect to Sellers in the Sharing and Gig Economy*"[282].

Especificamente sobre criptoativos, a OCDE tem tido papel igualmente importante no sentido de promover debates e apresentar soluções às problemáticas de sonegação e evasão fiscal. Em outubro de 2020 lançou relatório intitulado "*Taxing Virtual Currencies*"[283], indicando lacunas existentes a nível legislativo para os principais tipos de impostos, destacando a importância de concretizar guias claros, atualizados e consistentes sobre a incidência fiscal das criptomoedas em comparação com outros ativos. Já em seu relatório ordinário do mesmo período, em seguimento ao que já reportara em 2018[284], informou estar progredindo para a apresentação de estrutura de de-

---

281 Publicação intitulada "*The Sharing and Gig Economy: Effective Taxation of Platform Sellers: Forum on Tax Administration*"**.** Disponível em <URL:https://doi.org/10.1787/574b-61f8-en>, consult. 05.04.2022.

282 Disponível em <URL:https://www.oecd.org/ctp/exchange-of-tax-information/model-rules-for-reporting-by-platform-operators-with-respect-to-sellers-in-the-sharing-and-gig-economy.htm>, consult. 05.04.2022.

283 Disponível em <URL:https://www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.pdf>. Também em forma de *flyer* Disponível em <URL:https://www.oecd.org/tax/tax-policy/flyer-taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.pdf>, consult. 05.04.2022.

284 Tratou-se acerca da necessidade de estudos sobre criptomoedas e *blockchain* no contexto de digitalização na política e administração tributária, com desafios à política fiscal ao se considerar, por um lado, métodos novos e seguros de manutenção de registros e, de outro, riscos à transparência na cobrança de impostos sobre ganhos obtidos com tais ativos. Disponível em <URL:https://www.oecd.org/tax/OECD-Secretary-General-tax-report-G20-Finance-Ministers-Argentina-March-2018.pdf>, consult. 05.04.2022.

claração de impostos tendente a garantir transparência fiscal sobre criptoativos a ser aplicável pelos diversos países interessados[285].

Em janeiro de 2021, a OCDE apresenta novo relatório intitulado "*Regulatory Approaches to the Tokenisation of Assets*"[286], que tem como norte de atuação a proteção de investidores e consumidores financeiros, bem como salvaguardar a estabilidade financeira. Por isso, considerando a importância da *blockchain* e outras DLTs para os mercados financeiros, procura-se entender sua utilização e auxiliar na avaliação de suas implicações para promover cooperação e colaboração necessárias no desenvolvimento eficiente de respostas regulatórias.

Em 22 de março de 2022, conforme havia prometido, a OCDE apresentou documento de consulta pública intitulado "*Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*"[287]. Tratou-se de proposta de nova estrutura global de transparência tributária para fornecer relatórios e troca de informações sobre criptoativos, bem como propostas de alterações ao CRS para a troca automática de informações de contas financeiras entre países. Assim, pretendeu-se informar sobre a possível adoção de tal estrutura e seus componentes de design relacionados[288]. Após o recebimento de diversas contribuições, recentemente a OCDE apresentou a conclusão do seu trabalho[289].

Considera-se importante diante da circunstância de os criptoativos poderem ser explorados para minar as iniciativas internacionais de transparência fiscal existentes. Por isto, objetiva-se com esta estrutura, intitulada de CARF, a troca automática de informações fiscais relevantes sobre criptoativos entre administrações, abrangendo investimentos indiretos em criptoativos por meio de entidades de investimentos e derivativos. Também se alarga o âmbito do CRS aos produtos de moeda eletrônica e às CBDC's, bem como se procura melhorar os procedimentos de *due diligence* e os resultados dos relatórios, com vistas a aumentar a usabilidade das informações do CRS para as administrações fiscais e, sempre que possível, limitar os encargos para as Instituições Financeiras[290].

---

285 Disponível em <URL:https://www.oecd.org/tax/oecd-secretary-general-tax-report-g20-finance-ministers-october-2020.pdf>, consult. 05.04.2022.

286 Disponível em <URL:https://www.oecd.org/daf/fin/financial-markets/Regulatory-Approaches-to-the-Tokenisation-of-Assets.pdf>, consult. 05.04.2022.

287 Disponível em <URL:https://www.oecd.org/tax/exchange-of-tax-information/public-consultation-document-crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf>, consult. 05.04.2022.

288 Conforme noticiado em: <URL:https://www.oecd.org/tax/exchange-of-tax-information/oecd-seeks-input-on-new-tax-transparency-framework-for-crypto-assets-and-amendments-to-the-common-reporting-standard.htm>, consult. 05.04.2022.

289 Disponível em <URL:https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-tothe-common-reporting-standard.htm>, consult. 30.03.2023.

290 Idem.

5.3. OUTROS ATORES E INICIATIVAS INTERNACIONAIS

Enquanto iniciativas dignas de nota, destacam-se as diretrizes e linhas de ação designadas pelo Grupo Wolfsberg[291], a emergência da Convenção Multilateral (MLI – *Multilateral Instrument*) em matéria fiscal em substituição às Convenções sobre Dupla Tributação feitas entre países específicos[292] e a própria ideia de *Open Banking*, enquanto sistema financeiro aberto para compartilhamento de dados, produtos e serviços financeiros[293].

Da mesma forma se verifica a atuação da Organização Internacional de Valores Mobiliários (IOSCO)[294], que objetiva uniformizar as legislações sobre mercado de capitais pelo mundo. Por isso formulou documento intitulado "*IOSCO Objetives and Principles of Securities Regulation*"[295]. Conforme Grupenmacher[296], esta organização pauta sua atuação em três objetivos principais, quais sejam, "(i) proteção do investidor; (ii) garantia de um mercado justo, eficiente e transparente; e (iii) redução do risco sistêmico". Ainda que não tratem de criptoativos, demonstra-se a perspectiva colaborativa de construção de estruturas convergentes, com foco na harmonização legal de condutas.

---

[291] Disponível em <URL:https://www.wolfsberg-principles.com/about/current-priorities>, consult. 05.04.2022. Conforme seu sítio eletrônico, o Grupo Wolfsberg é uma associação de treze bancos globais que visa desenvolver estruturas e orientações para a gestão de riscos de crimes financeiros, particularmente no que diz respeito às políticas KYC, antilavagem de dinheiro e políticas contra o financiamento do terrorismo.

[292] Intitulada "Convenção Multilateral para a Aplicação das Medidas Relativas às Convenções Fiscais Destinadas a Prevenir a Erosão da Base Tributária e a Transferência de Lucros" e datada de 2016, tem como intuito uniformizar e padronizar a matéria acerca das regras de dupla tributação em âmbito fiscal, com vistas a substituir os acordos e convenções feitos de forma independente pelos diversos países. Disponível texto integral e em português na Internet: <URL:https://www.oecd.org/ctp/treaties/beps-multilateral-instrument-text-translation-portuguese.pdf>, consult. 05.04.2022.

[293] Conforme seu sítio eletrônico oficial no Brasil, trata-se de conjunto de regras e tecnologias que permite o compartilhamento de dados financeiros de clientes entre instituições financeiras e de pagamentos por meio da abertura e integração de seus respectivos sistemas. Assim, o projeto foi inspirado na experiência britânica, mas adaptado à realidade brasileira, e veio para dar mais transparência ao sistema financeiro nacional. Seu objetivo é fazer com que os consumidores tenham maior autonomia sobre a sua vida financeira e acesso a mais opções de produtos e serviços, com menos custos e mais transparência. Disponível em <URL:https://openbankingbrasil.org.br/2021/03/25/o-que-e-open-banking-2/>, consult. 05.04.2022.

[294] Conforme seu sítio eletrônico, foi criada em 1983. Seus membros regulam mais de 95% dos mercados de valores mobiliários do mundo em mais de 130 jurisdições: os reguladores de valores mobiliários em mercados emergentes respondem por 75% de seus membros comuns. Disponível em <URL: https://www.iosco.org/about/?subsection=about_iosco>, consult. 05.04.2022.

[295] Disponível em <URL:https://www.iosco.org/library/pubdocs/pdf/IOSCOPD561.pdf>, consult. 05.04.2022.

[296] Giovana Treiger Grupenmacher, *Op. Cit.*, pp. 98-99.

Destaque-se atuação específica da Interpol sobre criptoativos em reuniões ocorridas nos meses de março e outubro em 2018[297], quando se tratou acerca da emergência de uma plataforma global no combate a criminosos que buscam explorar a evolução das técnicas de anonimização. Reiterou-se a importância na capacitação e treinamento em *dark web* e criptomoedas para garantir que os investigadores acompanhem a evolução das ferramentas e técnicas forenses.

Por fim, destaquem-se pretensões recentemente trazidas pelo G20, com estabelecimento de padrões para um marco regulatório global de criptoativos, através de documentos a serem apresentados no corrente ano de 2023 pelo FSB (especificamente sobre stablecoins e mercados), FSB/FMI (tratando perspectivas macroeconômicas e regulatórias), FMI (com implicações da adoção generalizada de CBDCs) e BIS (nomeadamente questões analíticas, conceituais e mitigação de risco).

5.4. LEGISLAÇÃO REGIONAL EUROPEIA

Historicamente, diante da consolidação da ideia de livre circulação de bens, serviços e pessoas[298], e ainda do nível de globalização atingido, a legislação regional europeia demonstra ser pioneira em diversos aspectos da economia da sociedade digital[299], influenciando países de todo o mundo com suas iniciativas[300]. Tal não é diferente na criptoeconomia, em que o dito Efeito Bruxelas pode ser concretizado através da formulação de regulação que possa ser considerada paradigmática globalmente.

---

297 Conforme notícias disponíveis em seu próprio sítio eletrônico: <URL:https://www.interpol.int/News-and-Events/News/2018/INTERPOL-holds-first-DarkNet-and-Cryptocurrencies-Working-Group> e <URL:https://www.interpol.int/News-and-Events/News/2018/Challenges-of-Altcoins-for-investigations-prosecutions-focus-of-INTERPOL-meeting>, consult. 06.04.2022.

298 Que tem sua maior evolução através do Espaço Schengen, a qual conta atualmente com 26 (vinte e seis) países (22 dos quais são Estados-membros da União Europeia) e que, dentre outros aspectos, aboliram o controle de fronteiras internas. Para mais informações: <URL:https://ec.europa.eu/home-affairs/system/files_en?file=2020-09/schengen_brochure_dr3111126_pt.pdf>, consult. 07.04.2022.

299 Como exemplos recentes, as propostas de Lei dos Mercados Digitais (DMA ou *Digital Market Act*) para regular a prática dos gigantes da tecnologia e garantir mercados equitativos e abertos, e dos Serviços Digitais (DAS ou *Digital Services Act*) para estabelecimento de um espaço digital mais seguro; bem como do Regulamento do Parlamento e do Conselho sobre a Abordagem Europeia para a Inteligência Artificial.

300 A própria Lei Geral de Proteção de Dados Pessoais do Brasil (Lei 13.709/2018) foi criada com flagrante inspiração no Regulamento Geral sobre a Proteção de Dados da Europa (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho).

Inicialmente, de forma prudencial, tanto o Banco Central Europeu (BCE) em 2012[301] como a Autoridade Bancária Europeia (EBA) em 2013[302] já emitiam alertas sobre os riscos de investimentos realizados com criptomoedas, diante da ausência de regulação, supervisão e mecanismos legais de proteção do utilizador.

Ainda que este teor de alertas venha se seguindo nos últimos anos[303], já em maio de 2016 o Parlamento Europeu emitiu relatório sobre criptomoedas[304], através da Comissão dos Assuntos Econômicos e Monetários. Considera-se a viabilidade positiva de sua utilização, bem como da própria tecnologia subjacente (*blockchain* e demais DLTs), para o bem-estar dos cidadãos e o desenvolvimento econômico, nomeadamente no setor financeiro, mas para além dele, aumentando partilha de dados, transparência e confiança na relação entre cidadãos e governos e entre setor privado e clientes. Inclusive, reconhecendo potencialidades para ajudar os governos a reduzir branqueamento, fraude e corrupção, encoraja o teste da tecnologia para oferta de soluções administrativas. Por fim, solicita abordagem regulatória inteligente para favorecer a inovação e salvaguardar a integridade.

Além disso, verifica-se que a União Europeia acompanha de perto a evolução do uso da tecnologia *blockchain* ao criar, por iniciativa da Comissão, o *EU Blockchain Observatory and Forum*, responsável pela emissão de diversos estudos sobre o tema, destacando-se, no que tange ao tema específico de regulação, o relatório "*Legal and Regulatory Framework of Blockchains and Smart Contracts*", de 27 de setembro de 2019. Objetiva-se definir a real competência legislativa europeia, padronizar os entendimentos e interpretações sobre as temáticas envolvidas, estabelecer diálogos permanentes entre os setores público e privado, monitorar o desenvolvimento de tecnologias de uso menos maduras e utilizar a própria *blockchain* como ferramenta de regulamentação, dotando as instituições de mecanismos que possam, por exemplo, efetuar a identificação dos usuários da rede[305].

---

301 Intitulado "*Virtual Currency Schemes*". Disponível em <URL:https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, consult. 07.04.2022.

302 Intitulado "*Warning to Consumers on Virtual Currencies*". Disponível em <URL:https://www.eba.europa.eu/sites/default/documents/files/documents/10180/598344/b99b0dd0-f253-47ee-82a5-c547e408948c/EBA%20Warning%20on%20Virtual%20Currencies.pdf?retry=1>, consult. 07.04.2022.

303 A título de exemplo, a EBA (Autoridade Bancária Europeia), a ESMA (Autoridade Europeia dos Valores Mobiliários e dos Mercados) e a EIOPA (Autoridade Europeia dos Seguros e das Pensões Complementares de Reforma) emitiram alerta em 2018 para os riscos das moedas virtuais, num contexto de elevada volatilidade dos preços destas moedas. Para mais informações: <URL:https://www.bportugal.pt/comunicado/autoridades-de-supervisao-europeias-alertam-os-consumidores-para-os-riscos-das-moedas>, consult. 07.04.2022.

304 Disponível em <URL:https://www.europarl.europa.eu/doceo/document/A-8-2016-0168_PT.pdf>, consult. 07.04.2022.

305 Tom Lyons; Ludovic Courcelas; Ken Timsit, *Legal and regulatory framework of blockchains and smart contract* [Em linha], 2019, pp. 33-35, disponível em <URL:https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf>, consult.

Também merece registro o relatório chamado "*Advice Initial Coin Offerings and Crypto-Assets"*, da *European Securities and Markets Authority* (ESMA), publicada em janeiro de 2019[306], que busca auxiliar na identificação e enquadramento de certos criptoativos na legislação relacionada ao mercado de capitais[307].

Como primeiro documento europeu efetivamente regulatório sobre o assunto, tem-se a Diretiva (EU) 2018/843, do Parlamento Europeu e do Conselho[308], que alterou a Diretiva (UE) 2015/849, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo. Sujeitaram-se as *exchanges*, enquanto intermediadoras das operações com criptoativos, e as prestadoras de serviços de custódia de carteiras digitais, ao regramento vigente dos riscos considerados inerentes às operações ilícitas originárias do sistema financeiro e mercado de capitais. Tem-se como consequência a identificação de clientes e atividades suspeitas para efeitos de branqueamento de capitais ou financiamento ao terrorismo, tal como ocorre com as instituições financeiras tradicionais [309]. Ainda que não se almeje acabar com o anonimato, diante da possibilidade de realizar operações fora das plataformas ou sem custodiantes, foca-se no momento de conversão desses ativos em moedas fiduciárias e entrada no sistema bancário europeu[310].

10.06.2020. Disponível em <URL:https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf>, consult. 07.04.2022.

306 Disponível em <URL:https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf>, consult. 07.04.2022.

307 Para mais informações, v. Dayana de Carvalho Uhdre, *Op. Cit*., pp. 138-140, José Engrácia Antunes (2021a), *Op. Cit*., pp. 7-9, e José Engrácia Antunes (2021b), *Op. Cit*., pp. 192-196. Sobre a primeira, destaque-se o consenso de que "os criptoativos que reúnam as condições necessárias para serem qualificados como instrumentos financeiros deveriam ser regulamentados como tal", havendo sugestão de mudanças e acréscimos legislativos nos Estados-membros para responder adequadamente às características únicas do setor de criptoativos enquanto instrumentos financeiros e, assim, catalogar ofertas públicas ou outras atividades realizadas com criptoativos como sujeitas à supervisão prudencial específica da ESMA e autoridades nacionais competentes (p. 140).

308 Trata-se da 5ª Diretiva Anti-Lavagem de Dinheiro (AMLD5). Disponível em <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018L0843&from=PT>, consult. 07.04.2022. Concretizada no mesmo contexto do Regulamento (UE) 2018/1805 do Parlamento Europeu e do Conselho, relativo ao reconhecimento mútuo das decisões de apreensão e de perda (Nova Regra Européia de Confisco e Congelamento de Ativos Criminosos).

309 Feito conforme orientações do GAFI, porém se antecipando ao próprio guia de 2019, que sofreu recente atualização em 2021. Para uma análise comparativa entre esta Diretiva e as novas regras do GAFI: Lahis Kurtz; Florencia Lorenzo; Gustavo Rodrigues, "A regulação da União Europeia sobre criptomoedas e riscos de lavagem de dinheiro: uma análise crítica da Quinta Diretiva Antilavagem de Dinheiro frente aos provedores de serviços de criptomoeda" [Em linha], Instituto de Referência em Internet e Sociedade, Belo Horizonte, 2020, disponível em <URL:https://bit.ly/3cQIHM5>, consult. 07.04.2022.

310 Conforme se verifica na notícia abaixo, Disponível em <URL:https://www.europarl.europa.eu/news/pt/headlines/security/20180404STO00913/regras-mais-rigorosas-contra-o-branqueamento-de-capitais>, consult. 07.04.2022.

Após a eclosão da pandemia, a emergência regulatória do ambiente dos criptoativos fez antecipar o surgimento do conjunto de propostas ora em análise na União Europeia. De início, fora apresentado o intitulado Pacote Finança (ou Financiamento) Digital, apresentado pela Comissão em 24 de setembro de 2020. Nesse escopo foram apresentadas três proposituras: a Proposta de Regulamento em Mercados de Criptoativos (*Markets in Crypto Assets* - MiCA), a Proposta de Regulamento DLT[311] e a Proposta de Regulamento relativo à Resiliência Operacional Digital do setor financeiro (*Digital Operational Resilience Act* – DORA). Esta última passou a ter maior relevância pelo conflito entre Rússia e Ucrânia.

Diante da importância e impacto, destaque-se o MiCA, aplicável às pessoas que emitem criptoativos ou que prestam serviços de criptoativos na União Europeia, não enquadrados enquanto serviços financeiros[312]. Objetiva-se principalmente proteger os investidores, reproduzindo-se grande parte da legislação relativa aos instrumentos financeiros, de forma menos onerosa, com vista a promover a inovação, bem como proporcionar segurança jurídica e incorporar níveis adequados de integridade do mercado. Sobre *stablecoins*, face à sua pouca volatilidade, existem preocupações de salvaguarda da estabilidade financeira. Propõe-se padronização de operações e procedimentos, inclusive a taxonomia relacionada, o que dinamizará o desenvolvimento de negócios ao reduzir a complexidade e os custos para as empresas funcionarem no espaço territorial que abrange[313].

Aprovado recentemente perante o Parlamento Europeu e completado o processo legislativo com a adoção pelo Conselho da UE do quadro regulamentar, enquanto Regulamento (UE) 2023/1114, verificam-se importantes lacunas legislativas. Assim, não são abordados conclusivamente temas essenciais,

---

311 Relativo a um regime-piloto (*sandbox*) para as infraestruturas de mercado financeiro baseadas na tecnologia DLT, proporcionando ambientes baseados em automatização de processos, redução de custos e atuação ininterrupta (24/7). Esta foi a primeira proposta aprovada e já publicada enquanto Regulamento (UE) 2022/858 do Parlamento e do Conselho, de 30 de maio de 2022: <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R0858&from=PT>, consult. 16.07.2022.

312 Na Europa, são vários os arcabouços normativos aplicáveis aos serviços financeiros, destacando-se a Diretiva (2014/65) Europeia de Mercados e Instrumentos Financeiros (MiFID), o Regulamento (2014/600) dos Mercados de Instrumentos Financeiros (MiFIR), o regime de prospectos estabelecido pelo Regulamento dos Prospectos e a Diretiva dos Prospectos (Regulamento 2017/1129 e Directiva 2010/73), o Regulamento de Abuso de Mercado, a Diretiva (2013/50) Transparência e o Regulamento (2014/909) das Centrais de Valores Mobiliários.

313 Portanto, na classificação tripartite estabelecida neste trabalho, incluem-se os *tokens* de pagamento (inclusive *stablecoins*) e de utilidade, excluindo-se os de investimento. Além de outras exceções previstas, registre-se que a proposta de regulamento também não se aplica a entidades e pessoas específicas, com destaque para o BCE e bancos centrais nacionais dos Estados-membros (ao atuarem na qualidade de autoridades monetárias ou outras autoridades públicas), o Banco Europeu de Investimento, o Fundo Europeu de Estabilidade Financeira e Mecanismo Europeu de Estabilidade e organizações internacionais públicas.

como o universo DeFi e o grande volume de valores transacionados que estão operando à margem do regulador e com ausência de proteção dos usuários[314]; a existência de regime jurídico aos NFTs, tanto em relação a representações de ativos digitais como de ativos físicos; o registro de direitos e transações de direitos reais em sistemas de dados distribuídos, como já discorrido e existente em Liechtenstein quanto à possibilidade de tokenização da economia; e ainda a legitimidade e corpo jurídico às DAOs[315], evitando manter zona de penumbra ou de impunidade. Da mesma forma, há que se dar a devida importância ao aspecto da sustentabilidade ambiental do mercado[316].

Ainda dentro deste panorama regulatório, ressalte-se importante previsão no Quadro Europeu de Identidade Digital (Recomendação (UE) 2021/946 da Comissão Europeia), em que se propõe que os dados disponibilizados em DLTs sejam utilizados como prova qualificada em processos judiciais, proporcionando, portanto, maior valor no reconhecimento desta tecnologia.

Mais um conjunto de propostas fora apresentado pela Comissão em 20 de julho de 2021. Trata-se de pacote legislativo para reforma do regime europeu de combate ao branqueamento de capitais e ao financiamento do terrorismo (BCFT), em consonância com as últimas regras propostas pelo GAFI. Neste cenário são quatro os documentos veiculados: Regulamento que cria, em âmbito supranacional, a nova Autoridade para o Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo (AMLA); novo Regulamento que estabelece regras de prevenção da utilização do sistema financeiro para práticas BCFT, apresentado como *Single EU Rulebook*; Diretiva relativa aos mecanismos a criar pelos Estados-Membros para prevenir a utilização do

---

314 Para uma visão atualizada sobre este assunto, diante da problemática existente inclusive acerca do que pode ser considerado protocolo descentralizado, bem como soluções para alinhar tais aplicações com o quadro legislativo e a intervenção do Estado na economia, v. Guilherme Campos Maia e João Vieira dos Santos, "MiCA and DeFi ("Proposal for a Regulation on Market in Crypto-assets" and "Decentralised Finance")", *in Rev. Eletrónica de Direito* [Em linha], n° 2, Vol. 28, 2022, disponível em <URL:https://cij.up.pt/pt/red/edicoes-anteriores/2022-nordm-2/mica-e-defi-ldquoproposta-de-regulamento-sobre-mercados-de-criptoativosrdquo-e-financas-descentralizadasrdquo/>, consult. 30.03.2023.

315 *Decentralized Autonomous Organization* ou Organização Autônoma Descentralizada tem como norte de existência a definição de suas normas feita através de *smart contracts*, ou seja, de forma autoexecutável, sem atuação de um agente centralizador para tomada de decisões, permitindo (pretensamente) máxima transparência através principalmente da distribuição de *tokens* de governança para promover esta descentralização. Tanto o ecossistema de DeFi como as *exchanges* descentralizadas (DEX) são exemplos desta forma de organização, que não encontram na legislação europeia em exame reconhecimento de personalidade jurídica, o que impacta na atuação enquanto prestadoras de serviços.

316 Em votação recente, foi rejeitada proposta de eliminação de protocolos de consenso com alto consumo de energia, sobremaneira se está falando de *proof-of-work*, utilizado pelo *bitcoin*. Por outro lado e em consequência disto, foi aprovada previsão sobre a inclusão, até 1º de janeiro de 2025, da mineração de criptoativos entre as atividades econômicas contempladas na Taxonomia das Finanças Sustentáveis (Regulamento 2020/852), o que conduz à prestação de tais serviços de forma ambientalmente responsável.

sistema financeiro para efeitos de BCFT, de forma residual à proposta anterior; e Regulamento[317], em complemento ao MiCA e como resposta à regra de viagem do GAFI, que se propõe a revisar o Regulamento 2015/847 relativo às informações que acompanham as transferências de fundos.

No que concerne aos criptoativos, este conjunto de propostas objetiva combater o anonimato nas operações neste mercado, vinculando os prestadores de serviços em ativos virtuais à identificação específica dos envolvidos na respectiva transação. Também há especial tratamento às carteiras auto-hospedadas (ou seja, com custódia própria do usuário, portanto não fornecida por prestadores de serviços) no que concerne à rastreabilidade, à identificação e, sendo o caso, o bloqueio.

Por fim, em atenção à recente proposta da OCDE intitulada *Crypto-Asset Reporting Framework* (CARF), a Comissão Europeia apresentou a proposta de Diretiva (DAC-8) que procede à oitava alteração da Diretiva relativa à cooperação administrativa no domínio da fiscalidade (Diretiva 2011/16/EU), objetivando delinear regras de transparência fiscal para transações tomando por base relatórios de trocas de informações emitidos basicamente por provedores de serviços de criptoativos, em consonância com as novas regras do GAFI e com aplicação a partir de 1 de janeiro de 2026 caso aprovada.

6. SOBERANIA ESTATAL E MERCADO GLOBALIZADO

Verifica-se até então análise descritiva da importância do mercado de criptoativos, da visualização dos principais problemas decorrentes, do enfrentamento atualizado dos países mais relevantes para a temática, bem como o auxílio de organismos internacionais na consecução dos seus respectivos fins.

Em finalização do presente trabalho, apresenta-se nesta oportunidade visão explicativa para o fenômeno, com vistas a propor que a chave para melhor tratamento e ao menos minoração dos aspectos prejudiciais ao ambiente de negócios passa pela necessária superação do paradigma tradicional de soberania estatal, ao se priorizar ambiente colaborativo e conversações internacionais para apreender de forma mais adequada as nuances desse desafiador desenvolvimento tecnológico.

317 Conhecida como *Transfer of Funds Regulation* (TFR), fora aprovada em conjunto com o MiCA. Assim, trata-se do Regulamento (UE) 1023/1113.

6.1. PREMISSA DE BASE CRIMINOLÓGICA

Em termos de criminalidade no ambiente dos criptoativos, verifica-se crescente aumento tanto de investigações[318] quanto do próprio cometimento de crimes, o que influencia a garantia do investidor neste mercado, a exemplo da atuação de *hackers* que cometem cibercrimes em face das próprias empresas prestadoras de serviços[319].

Porém, considerando a importância da utilização de tais ferramentas tecnológicas, a exemplo do uso de criptomoedas como exercício de liberdade financeira pelas mulheres, remessa internacional de valores ou, mais comum, reserva de valor, o objetivo jamais deverá ser de regular para proibir, mas entender o funcionamento e o modo de uso para o enfrentamento dessa nova criminalidade cibernética. Conforme Bueno[320], cujo entendimento se coaduna com os demais delitos envolvidos, não se pode simplesmente criminalizar o seu uso, que, no delito de branqueamento de capitais, só é ilícito quando "empregado como instrumento no processo de disrupção da origem ilícita de patrimônio amealhado com a prática de infração penal anterior".

Na temática da criminalidade econômica e financeira, não somente organizações se aproveitam da fragilidade da máquina para ocultar cometimento de infração penal, mas também cidadãos comuns, no exercício de suas respectivas profissões, sobremaneira no ramo empresarial. Causam desequilíbrio econômico entre os participantes da respectiva atividade, prejudicam a livre concorrência e o desenvolvimento de profissionais que atuam de forma lícita no mercado.

Desta forma, para se verificar a efetividade no combate aos referidos delitos, necessário que se analise, além da legislação no dado território, o desenvolvimento de sólidas e concretas relações internacionais com outros países no intercâmbio de informações, através de convênios ou outras formas de cooperação transnacional, atuando de forma não somente repressiva, mas principalmente preventiva, tomando por base uma cultura forte de integridade e ética organizacional como balizadores das condutas dos líderes e das suas respectivas organizações. Justifica-se uma visão mais colaborativa entre os Estados, diante das consequências globais dos delitos e a possibilidade de deslocamento para jurisdições mais favoráveis à criminalidade.

Deste modo, importa registrar investigações de base criminológica para caracterização da criminalidade econômico-financeira relacionada às atividades e perceber como dissuadir os atores do cometimento desse tipo de delito.

---

318 Disponível em <URL:https://pplware.sapo.pt/criptomoeda/binance-maior-exchange-de-criptomoedas-investigada-por-crimes-fiscais/>, consult. 10.06.2020.

319 Tendência de crescimento de roubo de *bitcoin*: < https://exame.com/future-of-money/cybersecurity/roubo-de-btc-deve-crescer-em-2021-diz-relatorio-com-alerta-sobre-o-brasil/>. Acesso em: 10.06.2020.

320 Thiago Augusto Bueno, *Bitcoin e crimes de lavagem de dinheiro*, Campo Grande, Contemplar, 2020, p. 138.

Inicialmente, utilizando-se da perspectiva durkheimiana, Gonçalves e Andrade[321] (2019) verificam que a corrupção descoberta pela Operação Lava Jato é um fato social patológico presente na estrutura de diferentes órgãos e instituições que afeta a ordem social, decorrente de um estado de anomia no qual os indivíduos não aderem às normas sociais e morais vigentes.

Porém, utilizando-se do entendimento de Cruz[322], defende-se uma abordagem integrada ou a consumação de teorias específicas para analisar esta criminalidade econômico-financeira, pois a natureza, os danos e as vítimas revelam especificidades relativamente ao crime comum. Com isto, pode-se entender pela aplicabilidade ao menos parcial da Teoria da Associação Diferencial de Sutherland, pois esta cultura empresarial delituosa é transmitida aos sujeitos que trabalham nas organizações tal como qualquer conjunto de normas legais[323]; da Teoria da Anomia de Merton e seus competentes aperfeiçoamentos (anomia institucional e *strain*), que evidencia a desigualdade existente entre a estrutura social, cultural e econômica da sociedade[324]; e da Teoria da Escolha Racional de Becker, aperfeiçoada por Paternoster e Simpson, que incorpora as variáveis dos benefícios e dos custos do crime, dos princípios morais e dos fatores contextuais e situacionais como objeto de análise de custo-benefício para ponderação para o cometimento do delito, tendo em conta os possíveis benefícios que podem resultar da conduta e a possibilidade de ser punido[325].

Outro estudo científico bastante esclarecedor é o de Belo[326], que identificou que a evasão fiscal é uma prática comum entre os empreendedores e que costuma ser justificada por um somatório de fatores. São eles: baixa percepção do retorno dos tributos arrecadados por parte da gestão pública, percepção de impunidade e baixa fiscalização pelos órgãos de controle, e

---

321 Vinícius Batista Gonçalves e Daniela Meirelles Andrade, "A corrupção na perspectiva durkheimiana: um estudo de caso da Operação Lava Jato", *in Rev. Adm. Pública*, n° 2, Vol. 53, 2019, pp. 271-290, disponível em <URL:http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-76122019000200271&lng=en&nrm=iso>, consult. 18.01.2022.

322 José Neves Cruz, "A criminologia e o crime do colarinho branco", *In Infrações econômicas e financeiras: estudos de Criminologia e Direito,* AA.VV., Coimbra, Coimbra, 2013, pp. 50-63, especificamente na p. 61.

323 Inês Guedes e José Neves Cruz, "Infrações económicas e financeiras: aplicação da Teoria da Associação Diferencial de Sutherland", *In Infrações econômicas e financeiras: estudos de Criminologia e Direito,* AA.VV., Coimbra, Coimbra, 2013, pp. 88-101, especificamente na p. 99.

324 Tânia Dias e Rita Faria, "Anomia e infrações económicas e financeiras: o sucesso de uma teoria". *In Infrações econômicas e financeiras: estudos de Criminologia e Direito,* AA.VV., Coimbra, Coimbra, 2013, pp. 115-133, especificamente na p. 116.

325 Joana Veríssimo Maltez e José Neves Cruz, "A teoria da escolha racional e as infrações económicas e financeiras", *In Infrações econômicas e financeiras: estudos de Criminologia e Direito,* AA.VV., Coimbra, Coimbra, 2013, pp. 149-163, especificamente nas pp. 161-162.

326 Marina Emanuelli Belo, *Evasão fiscal em micro e pequenas empresas: reflexões sobre o comportamento empreendedor*, Dissertação (Mestrado em Administração), Universidade Tecnológica Federal do Paraná, Curitiba, 2019.

busca pela maximização dos rendimentos, principalmente como forma de sobrevivência dos negócios. Associando-se ao mau comportamento do empreendedor, para contornar as situações adversas que impedem a manutenção ou crescimento de sua empresa, utiliza intencionalmente a evasão fiscal como um jeito de obter os resultados desejados.

Por sua vez, Maragno, Knupp e Borba[327], através de análise qualitativa e quantitativa sobre a Operação Lava Jato, dispuseram sobre a compreensão dos vínculos que conectam os fraudadores e os seus cofraudadores em esquemas de corrupção e lavagem de dinheiro, demonstrando de forma numérica que os fraudadores líderes já haviam sido condenados anteriormente e/ou possuíam experiência nas fraudes cometidas, influenciando os demais membros da organização.

Por fim, Cusson[328] entende que "[a] abertura das fronteiras e a mundialização dos mercados estimulam o crescimento dos mercados criminosos internacionais", concluindo que estes mercados "prosperam e organizam-se nas lacunas do controlo social internacional e na esteira da mundialização da economia", sendo tais delitos "possíveis não apenas pela vulnerabilidade dos nossos mecanismos de regulação, mas também por força da prosperidade e das liberdades de que já não podemos abdicar". Uma destas "prosperidades" pode ser o desenvolvimento da criptoeconomia.

Assim, para evitar o cometimento de ilícitos, há que se dificultar a atuação do criminoso, seja incrustando uma cultura organizacional ética e transparente, diminuindo a transmissão de definições favoráveis à violação das leis, proporcionando valores sociais sólidos, extirpando as oportunidades ao delito, minorando os benefícios que podem resultar da conduta e/ou maximizando a possibilidade de punição.

6.2. EM DEUS CONFIAMOS, TODOS OS OUTROS DEVEM TRAZER DADOS[329]

Como outra premissa metodológica deste trabalho, há que se trazer não apenas argumentos de autoridade, mas comprovação estatística da opção fundada. Conforme disposto por Nunes[330] tratando sobre a temática da Jurimetria, "[o] Direito é um mecanismo de controle social que depende de uma aderência à realidade", devendo-se servir dos conhecimentos estatís-

---

327 L. M. D. Maragno; P. de S. Knupp; J. A. Borba, "Corrupção, lavagem de dinheiro e conluio no Brasil: evidências empíricas dos vínculos entre fraudadores e cofraudadores no caso Lava Jato", *in Rev. de Contabilidade e Organizações*, Vol. 13, 2019, pp. 5-18, disponível em <URL:http://www.revistas.usp.br/rco/article/view/158510>, consult. 27.11.2021.

328 Maurice Cusson, *Criminologia*, 3ª ed., Trad. Josefina Castro, Alfragide, Casa das Letras, 2011, pp.228-229.

329 No original, "*In God We Trust, All Others Must Bring Data*". Célebre frase de W. Edwards Deming.

330 Marcelo Guedes Nunes, *Jurimetria: como a Estatística pode reinventar o Direito*, 2ª ed., São Paulo, Thomson Reuters Brasil, 2019, disponível em <URL:https://proview.thomsonreuters.com/library.html#/library>, consult. 18.01.2022, RB-3.5.

ticos para controlar a incerteza e mensurar a probabilidade de sucesso dos argumentos, utilizando-se o Direito como fato social.

Por isto, sob uma perspectiva consequencialista, compreender o funcionamento de uma ordem jurídica consiste, basicamente, em entender os fatores que influenciam a produção das normas de regulação de condutas impostas pelo Estado, bem como monitorar a reação que essas normas provocarão nos seus destinatários. Desta forma, a Jurimetria tem como objeto a investigação do funcionamento da ordem jurídica, que tem por objetivo influenciar o comportamento humano[331].

Em uma perspectiva de natureza indutiva, ainda que diversos Estados tentem regular o ambiente dos criptoativos, está-se diante de forma limitada principalmente em matéria de território. Neste cenário proposto, através da coordenação, colaboração e cooperação entre os entes nacionais e internacionais, as experiências exitosas poderão ser melhor desenvolvidas e servir como base e modelo de atuação.

Conforme Bueno[332], destaque-se que simplesmente banir este mercado não possui eficácia, diante do seu caráter descentralizado, difuso e transnacional. Concluindo pela necessidade de regulação, concorda-se com o referido autor quando explicita que "tal processo deve ser feito com amplo debate, do qual participem agentes do Estado, desenvolvedores de tecnologia e usuários, de modo a conferir legitimidade e aplicabilidade efetiva".

Orienta-se pelas propostas da OCDE e da União Europeia já veiculadas, bem como a previsão, contida na Convenção Multilateral Fiscal (MLI – *Multilateral Instrument*) em substituição às atuais convenções bilaterais sobre dupla tributação[333], acerca dos acordos de trocas de informações entre Estados, com base nos princípios da transparência, reciprocidade e proporcionalidade.

Entende-se que os empreendedores acabam buscando jurisdições que dispõem de orientações sobre as normas e consequentes obrigações cabíveis às diversas operações com criptoativos, ainda que sejam dispostas e previstas de modo infralegal, como regulamentos, instruções ou até recomendações, a exemplo da Suíça, que atualmente dispõe de regulação ampla sobre a matéria.

Assim, há que se privilegiar segurança jurídica a todos os envolvidos, com trocas de informações mais automatizadas e padronizadas aos níveis de exigência de identificação dos usuários e obrigações às empresas para garantir segurança aos investidores, através de dispositivos proporcionais e com abrangência internacional.

Por isso, entendendo o fenômeno como uma disrupção tecnológica e financeira, com a possibilidade real e futura de uma economia tokenizada,

---

331 Marcelo Guedes Nunes, *Op. Cit*., RB-5.2.

332 Thiago Augusto Bueno, *Op. Cit*., p. 138.

333 Para mais informações sobre o tema, v. Glória Teixeira, *Op. Cit*., pp. 300-312.

conclui-se pela afetação em diversas áreas, como o mercado securitário, financeiro, da tributação, de registro de propriedade intelectual e de dados, o que enseja a importância de visão ampliada, inclusive além do paradigma tradicional de soberania estatal.

6.3. EMERGÊNCIA DE PERSPECTIVA COLABORATIVA E DIÁLOGO SUPRANACIONAL

Quando se fala de regulação, fala-se de ordem e poder. Dentro dessa lógica de regulação governamental e estatal, verifica-se como uma tendência mundial tentar diminuir as externalidades negativas, os riscos que alguns comportamentos podem acarretar para o sistema jurídico de uma forma ampla. Por isso, adequada a participação máxima no debate regulatório, para proporcionar maior segurança jurídica, ainda que em detrimento da possibilidade de funcionamento autorregulado do setor[334], que, admite-se, teria potencialmente capacidade para lançar novos projetos com maior agilidade.

Assim, o esforço científico-acadêmico deste estudo também tem como norte de atuação o comportamento organizacional dos líderes das instituições, no sentido de influenciá-los ou mesmo compeli-los à consecução da necessária mudança da cultura de suas empresas, proporcionando a alteração do mau comportamento neste contexto.

Conforme Ross[335], depois do eBay e da economia de compartilhamento (ou de partilha) como Airbnb, está-se diante de mais um desdobramento da codificação da confiança, em que o intuito da tecnologia digital é de substituição de bancos e governos "como árbitros de confiança e de criar um novo protocolo para a realização de negócios em todo o mundo".

Igualmente se verifica em Telles[336] a visualização dessa descentralização da economia, que se transmuda em virtual e está inserida em um mundo sem fronteiras. Tal impacta inclusive o sistema tributário global estabelecido pela OCDE, baseado na soberania para rastreamento de dados e ativos de indivíduos e organizações no sistema financeiro. Porém, como estabelecer um sistema tributário internacional nesse mundo virtual, sem soberania e sem sistema financeiro?

Antonopoulos[337] demonstra a importância desse ramo de negócios ao tratar especificamente do *bitcoin*, aplicável à criptoeconomia. Para tanto, foca na dificuldade de penetração das instituições bancárias em lugares mais longínquos, ao passo que o acesso à internet e, consequentemente, à rede

---

334 Sobre *soft law* e autorregulação, v. João Vieira dos Santos, "Soft Law e boa governança no mercado das criptomoedas", *in Rev. Eletrônica de Direito* [Em linha], n° 2, Vol. 16, 2018, disponível em <URL:https://cije.up.pt/client/files/0000000001/9_589.pdf>, consult. 16.07.2022.

335 Alec Ross, *As indústrias do futuro*, Coimbra, Conjuntura Actual Editora, 2016, p. 1743.

336 Christiana Mariani da Silva Telles, *Op. Cit.*, pp. 43-44.

337 Andreas M Antonopoulos, *The internet of Money* [Em linha], Merkle Bloom LLC, [S. l.], 2017, p. 85.

de telefonia móvel, supera até mesmo o contingente populacional com acesso à água potável. De forma genuína, entende que a revolução ocasionada pelas criptomoedas teria o intuito de inovação e de quebrar paradigmas, até mesmo retirando o público consumidor do sistema bancário, ao comparar tal atividade com um aplicativo.

Todavia, as tentativas de regulamentos nacionais têm se configurado como fragmentadas e em evolução, com coordenação e consistência limitada[338], o que gera preocupações em vários setores que são atingidos pelo fenômeno[339]. Verificam-se diferenças relevantes de interpretação nas questões mais basilares do setor, como a taxonomia e natureza jurídica das espécies de criptoativos, o que impacta na respectiva tributação e na inserção destes, por exemplo, sob a legislação de mercado de capitais[340].

Como consequência, dependendo do país de residência dos usuários, as próprias *exchanges* adotam tratamentos legais diferentes, o que impacta na insegurança jurídica e na existência de dificuldades ou mesmo entraves ao desenvolvimento dos serviços prestados. Em Grupenmacher[341] há exemplo claro através da empresa presente em 42 (quarenta e dois) países, que expressa preocupação quanto à localização do destinatário do serviço. Por exemplo, dispõe que apenas aos usuários da União Europeia se aplicam previsões relacionadas a serviços com *e-money*.

De todo modo, é inconteste o protagonismo atingido nos últimos anos[342], ao ponto de mais de 100 (cem) bancos centrais nacionais estarem em distintas etapas de análise e até experimentação de suas respectivas moedas digitais (CBDC's)[343]. Não se pode também perder de vista que a tecnologia subjacente (*blockchain*) se encontra em franca expansão, tendo em vista a

---

338 A Europa, por exemplo, mesmo após aprovação dos projetos em discussão, padecerá de lacunas legislativas.

339 O Comitê de Basileia, por exemplo, publicou em junho de 2022 documento de consulta sobre exposições de bancos aos criptoativos. Disponível em <URL:https://www.bis.org/bcbs/publ/d533.pdf>, consult. 13.07.2022.

340 Em relação às criptomoedas enquanto criptoativo mais difundido, verificam-se diferenças gritantes, como em "*Cryptocurrency Regulations Around the World*". Disponível em <URL:https://complyadvantage.com/blog/cryptocurrency-regulations-around-world/>. Inclusive verificam-se dezenas de países que, de forma parcial ou absoluta, baniram o uso de criptomoedas em seus respectivos territórios, conforme se verifica nas pp. 66-67 do documento "*Regulation of Cryptocurrency Around the World: November 2021 Update*". Disponível em <URL:https://tile.loc.gov/storage-services/service/ll/llglrd/2021687419/2021687419.pdf>, consult. 11.07.2022.

341 Giovana Treiger Grupenmacher, *Op. Cit*., p. 149.

342 A JP Morgan já atua no setor de tokenização de ativos para DeFi. Disponível em <URL:https://www.coindesk.com/business/2022/06/11/jpmorgan-wants-to-bring-trillions-of-dollars-of-tokenized-assets-to-defi/?outputType=amp>, consult. 13.07.2022.

343 Conforme se verifica em recente publicação da *Visa Economic Empowerment Institute*. Disponível em <URL:https://usa.visa.com/content/dam/VCOM/regional/na/us/sites/documents/veei-the-art-of-public-money.pdf>, consult. 13.07.2022.

multiplicidade de aplicações além do ramo de negócios em análise, inclusive no meio ambiente[344] e até mesmo no setor público[345].

Ressalte-se que a obrigatoriedade de licenciamento para atuação em dado território não elimina o problema, podendo até aprofundá-lo ou causar entraves ao desenvolvimento das novas tecnologias, diante de possíveis diferenças obrigacionais a cada autorização para atuar, o que releva igualmente para fins fiscais, de garantias de investimento e sustentabilidade do setor, bem como dificuldades de fiscalização em uma economia digital totalmente globalizada.

Com isso, levando-se em conta a necessidade de conversações transconstitucionais, utilizando a nomenclatura de Neves[346], no sentido de entrelaçamentos como pontes de transição entre sistemas jurídicos diversos, ao desenvolvimento de racionalidades transversais específicas, surgiram diversos textos, normas e recomendações, por parte de organizações internacionais, com o objetivo de auxiliar na regulamentação de tais atividades.

Em realidade, identificam-se problemas comuns neste ramo de negócios em circunstâncias nunca antes vivenciadas. Não se está a tratar de fatos jurídicos que ocorrem igualmente em espaços territoriais distintos, como normalmente se verifica na economia globalizada, a exemplo dos aplicativos de economia compartilhada como Uber. Em realidade, está-se diante da possibilidade de um mesmo produto, de origem comum, atingir indistintamente pessoas e organizações em todo o mundo, independente dos limites territoriais dos envolvidos.

Problemas são descobertos e potencializados nesta nova economia, nomeadamente o pseudoanonimidade dos criptoativos, a jurisdição aplicável aos casos concretos e a descentralização das redes *blockchain*, inclusive com definição de critérios claros sobre a caracterização do que é efetivamente descentralizado, considerando o universo DeFi e atuação das DAOs.

Some-se a isto a circunstância de que as opções legislativas analisadas ainda primam pelo papel centralizador de informações dos diversos tipos de prestadores de serviços no setor, desafio que pode ser potenciado quando da identificação, fiscalização e regulação de negócios puramente descentra-

---

344 Por exemplo, artigo disponível em <URL:https://corpgov.law.harvard.edu/2022/06/30/the-impact-of-technology-on-climate-oversight-what-board-directors-need-to-know/>, consult. 13.07.2022.

345 O Estado Colombiano lançou guia de referência para implementação de projetos com tecnologia *blockchain*: <URL:https://drive.google.com/file/d/1wwiS8XSu4xLdkwhzW0w7D_7jmY7G_tpW/view>, consult. 13.07.2022.

346 Marcelo Neves, *Transconstitucionalismo*, São Paulo, Martins Fontes, 2009, p. 62. Ciente da diferença doutrinária entre constitucionalismo transnacional, que preconiza uma única ordem constitucional para diversos Estados e o transconstitucionalismo de Neves, que reconhece problemas comuns a diversas ordens para se chegar a denominador comum que resolva a questão apresentada, neste trabalho, diante da limitação dos seus objetivos, foca-se nesta segunda perspectiva.

lizados. Inclusive as próprias propostas européias em discussão objetivam proteção de investidores e estabilidade financeira igualmente levando em consideração o protagonismo destes atores que fazem as vezes de intermediários. Realidade esta que em futuro não tão distante poderá se configurar em sua maioria por transações verdadeiramente desintermediadas (P2P).

Deste modo, impõe-se a necessidade de superar o paradigma tradicional de soberania secular, abrindo-se a possibilidade trazida por Vita[347] da intitulada tração estrutural como elemento fundamental do ponto de vista sistêmico, dispondo que "sistemas jurídicos distintos podem (re)produzir estruturas similares a partir de um processo de evolução convergente e paralela".

O desafio a ser enfrentado, utilizando-se das razões de Grupenmacher[348], "é encontrar um equilíbrio entre a regulação, a segurança jurídica e os riscos atrelados à inovação". Dito de outra forma, deve-se privilegiar a necessária regulação ao ambiente de negócios, porém sem impedir o desenvolvimento e evolução de novas tecnologias e o próprio mercado de criptoativos, ou seja, no controle legal que deve existir sobre criptoativos deverá ser encontrado um bom equilíbrio entre esse efetivo controlo e a liberdade para os vários agentes inovarem dentro deste mercado em constante mudança.

E isto poderá ser conseguido ao se proporcionar ambiente de diálogo supranacional. Até porque, utilizando-se das razões de Meira, Dall'ora e Santana[349] acerca das criptomoedas, circunstância aplicável à criptoeconomia como um todo, reitera-se que a importância global não respeita barreira física estatal e um mesmo negócio possui "real capacidade de estar em qualquer lugar do mundo ao mesmo tempo". Concluindo a visão doutrinária acima, deve-se "debruçar sobre uma matéria econômica e trabalhar juntos para entender, aplicar e operacionalizar" o ambiente de negócios maneira equilibrada e coesa.

Há que se estabelecer um espaço de diálogo multifacetado com os principais *players*, administradores e administrados, entendendo-se pela alteração do paradigma de regulação. Tanto no sentido de promover conversações diretas com os empreendedores como igualmente por se entender que a normatização eminentemente nacional não resolve os problemas enfrentados, sobremaneira considerando a falta de padronização de entendimentos e obrigações acessórias, insegurança jurídica nas relações entre os envolvidos e limitação de abrangência dos diplomas. Além de se considerar a possibilidade de deslocamento para jurisdições mais favoráveis à ilegalidade, em verdadeira corrida de gato e rato existente no combate à criminalidade econômica.

---

347 Jonathan Barros Vita, *Op. Cit*., p. 303.

348 Giovana Treiger Grupenmacher, *Op. Cit*., p. 98.

349 Liziane Angelotti Meira, Fillipe Soares Dall'ora e Hadassah Laís S. Santana, *Op. Cit*., pp. 354-355.

Ao se fomentar o crescimento da economia, não se pode negligenciar a necessidade de garantir segurança de quem está atuando neste nicho. Seja para empreender regulação que promova a higidez do sistema financeiro e monetário; que reduza a incidência de fatos criminosos relacionados ao uso de criptoativos; que possibilite garantias e proteção aos investidores; e que promova a justa e proporcional tributação das manifestações de riqueza, tanto no sentido de determinar a natureza jurídica das relações tributárias como para garantir fiscalização efetiva no cenário internacional. Por fim, também devem ser vislumbradas medidas que se traduzam em garantir o desenvolvimento sustentável através do privilégio à utilização de fontes de energia renováveis e limpas.

7. CONSIDERAÇÕES FINAIS

O presente trabalho foi iniciado através da demonstração, sob aspectos históricos e econômicos, da pujança e potencialidade do mercado de criptoativos, com cifras que podem impactar diversos ambientes de negócios. Isto considerando as criptomoedas enquanto espécie mais conhecida, porém igualmente considerando o poder inovador dos NFT's, das finanças descentralizadas (DeFi) e dos *smart contracts*, acompanhados pelas *stablecoins* e CBDC's enquanto mecanismos de estabilização e maior confiança no mercado, seguindo-se pelo potencial da tokenização de ativos para o futuro da economia digital.

Ao se verificar este contexto, identificam-se problemas em dimensão global, quais sejam, facilidade para cometimento de ilícitos (sobremaneira branqueamento de capitais, fraude e evasão fiscal), dificuldade de fiscalização e tributação das manifestações de riqueza, importância da proteção dos investidores no desenvolvimento dos serviços prestados, promoção de higidez do sistema financeiro e monetário, e respeito à sustentabilidade e responsabilidade socioambiental para o setor.

À sua maneira, são vários os países que têm tentado regular as diversas matérias envolvidas, sendo analisadas, ainda que brevemente, o formato de legislação empreendida, observando-se desde previsão de curso legal do *bitcoin* (El Salvador) até a total proibição de tal comercialização (China), passando pelo entendimento contraditório de órgãos estatais dentro de um mesmo país (Estados Unidos da América), pela instituição da primeira CBDC que se tem notícia, lastreada em *commodities* nacionais (Venezuela), pelas primeiras experiências autônomas européias (Suíça, Malta e Liechtenstein) e pelos desenvolvimentos em ambiente asiático (Japão e Singapura). Por fim, dedica-se especial atenção ao tratamento legal existente no Brasil e em Portugal.

Diante da identificação de problemas comuns em âmbitos diferentes da vida em sociedade, naturalmente são verificados documentos originários de

organismos internacionais que tentam, na perspectiva que são constituídos, auxiliar no desenvolvimento de soluções exequíveis e eficientes. Destacam-se a Convenção de Budapeste sobre crimes cibernéticos, as orientações do GAFI acerca da prevenção ao branqueamento de capitais e financiamento ao terrorismo, o entendimento da OCDE em matéria tributária e ainda o conjunto de medidas legislativas instituídas pela União Europeia para proporcionar padronização e segurança jurídica ao setor, sobremaneira o MiCA.

Abordadas as circunstâncias acima apontadas, ainda que de forma limitada e sem o objetivo de esgotar o tema, privilegiando metodologia de análise holística e descritiva para demonstrar a complexidade do setor, utilizou-se tanto a dedução como a indução enquanto métodos de abordagem.

Dedutivamente, tomaram-se premissas básicas para maior concentração na temática proposta, dialogando entre o estado da arte das regulações existentes e a necessidade de superação do paradigma tradicional de soberania dos Estados para uma perspectiva colaborativa de ordem supranacional. Indutivamente, com premissa de ordem criminológica e levando em consideração a análise jurimétrica do fenômeno para bem compreendê-lo, faz-se proposição universal e necessária que se estabelece pelo exame do maior número possível de objetos relacionados ao objetivo proposto, com tomada de posições conclusivas.

Conclui-se que as tentativas de regulamentos nacionais têm se configurado como fragmentadas e em evolução, com coordenação e consistência limitada, o que gera preocupações em vários setores que são atingidos pelo fenômeno. Verificam-se diferenças relevantes de interpretação nas questões mais basilares do setor, como a taxonomia e natureza jurídica das espécies de criptoativos, o que impacta na respectiva tributação e na inserção destes, por exemplo, sob a legislação de mercado de capitais. Inclusive, a obrigatoriedade de licenciamento para atuação em dado território não elimina o problema, podendo até aprofundá-lo ou causar entraves ao desenvolvimento das novas tecnologias.

Estando-se genuinamente inserido em mercado que possibilita que um mesmo produto, de origem comum, atinja indistintamente pessoas e organizações em todo o mundo, independente dos limites territoriais dos envolvidos, impõe-se a necessidade de superar o paradigma tradicional de soberania secular. Deve-se privilegiar a necessária regulação ao ambiente de negócios, porém sem impedir o desenvolvimento e evolução de novas tecnologias e o próprio mercado de criptoativos, com foco em perspectiva de diálogo supranacional e multifacetado entre os diversos *players* envolvidos, pois, ao se fomentar o crescimento da economia, não se pode negligenciar a necessidade de garantir segurança de quem está atuando neste nicho.

Enquanto estudo primordialmente descritivo do autor, necessariamente haverá continuidade desta investigação. Tem-se como norte de atuação futura o amadurecimento da perspectiva regulatória internacional, com hipótese na padronização de condutas, exigências e obrigações, baseado em

balizas mínimas de interpretação e aplicabilidade dos cenários de implementação de novas tecnologias a serem desenvolvidas, tendo em vista o mercado estar em constante expansão, mutação e diferenciação.

8. BIBLIOGRAFIA

Aguillar, Fernando Herren, *Direito Econômico: do direito nacional ao direito supranacional*, São Paulo, Atlas, 2006.

Amaro, Luciano, *Direito tributário brasileiro* [Em linha], 24ª ed., São Paulo, Saraiva Educação, 2021, disponível em <URL:https://integrada.minhabiblioteca.com.br/#/books/9786555592993/>, consult. 02.01.2022.

Amorim; Lucas de Lima Carvalho Pedro, "A tributação dos jogos eletrônicos no Brasil: perspectivas e desafios", *In Direito e Novas Tecnologias* [Em linha], Costa-Corrêa, André; Predolim, Emerson Alvarez; Longhi, Maria Isabel Carvalho Sica; Rebouças, Rodrigo Fernandes, São Paulo, Almedina Brasil, 2020, pp. 315-358, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 02.01.2022.

Andrade, Mariana Dionísio de, "Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro", *in Rev. Bras. de Políticas Públicas* [Em linha], n° 3, Vol. 7, 2017, disponível em <URL:https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4897/3645>, consult. 24.12.2021.

Antonopoulos, Andreas M, *The internet of Money* [Em linha], Merkle Bloom LLC, [S. l.], 2017.

Antunes, José Engrácia (2021a), *As Criptomoedas* [Em linha], 2021, disponível em <URL:https://portal.oa.pt/media/133308/jose-engracia-antunes.pdf>, consult. 12.07.2022.

Antunes, José Engrácia (2021b), *A Moeda – Estatuto Jurídico e Econômico*, Coimbra, Almedina, 2021.

Belo, Marina Emanuelli, *Evasão fiscal em micro e pequenas empresas: reflexões sobre o comportamento empreendedor*, Dissertação (Mestrado em Administração), Universidade Tecnológica Federal do Paraná, Curitiba, 2019.

Bottini, Pierpaolo Cruz; Badaró, Gustavo Henrique, *Lavagem de dinheiro: aspectos penais e processuais penais: comentários à Lei 9.613/1998, com as alterações da Lei 12.683/2012*, São Paulo, Revista dos Tribunais, 2016.

Braga, Romulo Rhemo Palitot, *Lavagem de dinheiro: fenomenologia, bem jurídico protegido e aspectos penais relevantes*, 2ª ed., Curitiba, Juruá, 2013.

Brasil, Receita Federal, "Instrução Normativa 1.888/2019, alterada pela Instrução Normativa 1.899, de 10 de julho de 2019" [Em linha], DOU 07 Maio 2019, disponível em <URL:http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592>, consult. 27.02.2022.

Brasil, Tribunal de Contas da União, "Levantamento da tecnologia blockchain" [Em linha], 2020, disponível em <URL:https://portal.tcu.gov.br/data/files/59/02/40/6E/C4854710A7AE4547E18818A8/ Blockchain_sumario_executivo.pdf>, consult. 27.11.2021.

Bueno, Thiago Augusto, *Bitcoin e crimes de lavagem de dinheiro*, Campo Grande, Contemplar, 2020.

Callegari, André Luís, *Lavagem de Dinheiro* [Em linha], 2ª ed. rev., atual. e ampl., São Paulo, Atlas, 2017, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9788597012293/>, consult. 23.12.2021.

Camacho, Tatiana Silveira; Silva, Guilherme Jonas Costa da, "Criptoativos: Uma Análise do Comportamento e da Formação do Preço do Bitcoin", *in Rev. de Economia da Universidade Federal do Paraná* [Em linha], n° 68, Vol. 39, 2018, disponível em <URL:https://revistas.ufpr.br/economia/article/view/67885>, consult. 24.12.2021.

Carrazza, Roque Antonio, *Curso de Direito Constitucional Tributário*, São Paulo, Malheiros, 2013.

Carvalho, Mariana Pimenta Ferreira de, *Criptomoedas: alguns problemas de regime,* Dissertação (Mestrado em Direito), Faculdade de Direito da Universidade do Porto, Porto, 2021.

Carvalho, Paulo de Barros, *Curso de direito tributário*, 10ª ed., São Paulo, Saraiva, 1998.

Carvalho, Sara Campelo Rocha Areia de, *Bitcoin: Do Enquadramento Jurídico à Tributação*, Dissertação (Mestrado em Direito), Universidade Católica Portuguesa, Porto, 2018.

Castagna; Ricardo Alessandro, "Blockchain e operações financeiras: impactos na tributação", *In Direito e Novas Tecnologias* [Em linha], Costa-Corrêa, André; Predolim, Emerson Alvarez; Longhi, Maria Isabel Carvalho Sica; Rebouças, Rodrigo Fernandes, São Paulo, Almedina Brasil, 2020, pp. 555-590, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 02.01.2022.

Chirinos, Gabriel Alejandro, "Regulación y Tributación en el Mercado de Criptoactivos, una Perspectiva de Derecho Comparado", *in Rev. de la Facultad de Derecho Montevideo* [Em linha], n° 48, 2020, disponível em <URL: https://perma.cc/3TNK-8ZEZ>, consult. 30.01.2022.

Chishti, Susanne; Barberis, J., *A Revolução Fintech: o manual das startups financeiras* [Em linha], Rio de Janeiro, Alta Books, 2017, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786555206760/>, consult. 27.11.2021.

Coêlho, Sacha Calmon Navarro, *Curso de Direito Tributário Brasileiro* [Em linha], 17ª ed., Rio de Janeiro, Forense, 2020, disponível em <URL: https://integrada.minhabiblioteca.com.br/#/books/9788530988357/>, consult. 02.01.2022.

Conselho da Europa, "Convenção de Budapeste sobre o Cibercrime" [Em linha], Comitê Europeu para os Problemas Criminais, 2001, disponível em <URL: https://rm.coe.int/16802fa428>, consult. 05.04.2022.

Cruz, José Neves, "A criminologia e o crime do colarinho branco", *In Infrações económicas e financeiras: estudos de Criminologia e Direito,* AA.VV., Coimbra, Coimbra, 2013, pp. 50-63.

Cusson, Maurice, *Criminologia*, 3ª ed., Trad. Josefina Castro, Alfragide, Casa das Letras, 2011.

Dias, Tânia; Faria, Rita, "Anomia e infrações económicas e financeiras: o sucesso de uma teoria". *In Infrações econômicas e financeiras: estudos de Criminologia e Direito,* AA.VV., Coimbra, Coimbra, 2013, pp. 115-133.

Diniz, Bruno, *O Fenomeno Fintech: tudo sobre o movimento que está transformando o mercado financeiro no Brasil e no mundo* [Em linha], Rio de Janeiro, Alta Books, 2020, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9788550815459/>, consult. 27.11.2021.

Duarte, Paulo, "Obrigações de Dinheiro (Obrigações monetárias) e Obrigações de Bitcoins. Estudos de Direito do Consumidor" [Em linha], n° 14, 2018, pp. 343-381, disponível em <http://www.rdmf.es/wp-content/uploads/2018/09/Paulo-Duarte-art%C3%ADculo.pdf>, consult. 30.03.2023.

Dumbra, Bruno de Morais, "Sequestro de dados e terrorismo digital: os atuais tipos penais são suficientes para punir os crimes em ambiente virtual?", *In Direito e Novas Tecnologias* [Em linha], São Paulo, Almedina Brasil, 2020, pp. 73-88, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 23.12.2021.

Eco, Umberto, *Como se faz uma tese em Ciências Humanas*, 19ª ed., Trad. Ana Falcão Bastos e Luís Leitão, Lisboa, Editorial Presença, 2015.

El Salvador, "Ley Bitcoin" [Em linha], Assembleia Legislativa de El Salvador, 2021, disponível em <URL:https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/27F0BD6F-3CEC-4F52-8287-432FB35AC475.pdf>, consult. 26.01.2022.

Estellita, Heloisa, "Criptomoedas e lavagem de dinheiro", *in Rev. Direito FGV* [Em linha], n° 1, Vol. 16, 2020, disponível em <URL:https://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/issue/view/4501/2488>, consult. 24.12.2021.

Eublockchain, "European Union Comission. Legal and Regulatory Framework of Blockchain and Smart Contracts" [Em linha], Setembro de 2019, disponível em <URL:https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf>, consult. 27.11.2021.

Europol; European Monitoring Centre for Drugs and Drug Addiction, "Drugs and the darknet: Perspectives for enforcement, research and policy" [Em linha], 2017, disponível em <URL:https://cryptographybuzz.com/cryptocurrency-laundered-bitcoin/>, consult. 24.12.2021.

Fatf, "Guidance for a Risk-Based Approach to Virtual Assets And Virtual Asset Service Providers" [Em linha], FATF, Paris, 2019, disponível em <URL:https://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html>, consult. 05.04.2022.

—, "Updated Guidance for a Risk-Based Approach to Virtual Assets And Virtual Asset Service Providers" [Em linha], FATF, Paris, 2021, disponível em <URL:https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>, consult. 05.04.2022.

—, "International Standards on combating Money laudering and the financing of terrorism & proliferation" [Em linha], The FATF Recommendations, FATF, Paris, 2012-2022, disponível em <URL:https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>, consult. 05.04.2022.

Feio, Diogo Nuno de Gouveia, *O Governo, o Orçamento e os Impostos: Uma história interminável entre a União Europeia e a União Económica e Monetária*, [S. l.], Petrony, 2020.

Feitosa, Maria Luiza Pereira de Alencar Mayer, *Paradigmas inconclusos: os contratos entre a autonomia privada, a regulação estatal e a globalização dos mercados,* Coimbra, Coimbra, 2007.

Florêncio Filho, Marco Aurélio; Castanheira, Yasmin Abrão Pancini, "Prevenção à Lavagem de Dinheio em Cryptocurrencies Exchanges" *In Direito Penal Econômico* [Em linha], Cury, Rogério, São Paulo, Almedina, 2020, pp. 105-130, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556270531/>, consult. 23.12.2021.

Fujihira, Katsuhiko; Graham, Seth M., "Japanese Cryptocurrency Update: New Amendments to Crypto Asset Regulations Take Effect May 1" [Em linha], Abr. 2020, disponível em <URL://www.mofo.com/resources/insights/200423-japanese-cryptocurrency-update.html>, consult. 13.02.2022.

Ghirardi, Maria do Carmo Garcez, *Criptomoedas: aspectos jurídicos* [Em linha], São Paulo, Almedina Brasil, 2020, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556270364/>, consult. 27.11.2021.

Gomes, Daniel de Paiva, *Bitcoin: a tributação de criptomoedas: da taxonomia camaleônica à tributação de criptoativos sem emissor identificado*, São Paulo, Revista dos Tribunais, Thomson Reuters Brasil, 2021.

—, *Bitcoin: a tributação de investimentos em criptomoedas*, Dissertação (Mestrado em Direito), Fundação Getúlio Vargas, São Paulo, 2019.

Gonçalves, Vinícius Batista, e Andrade, Daniela Meirelles, "A corrupção na perspectiva durkheimiana: um estudo de caso da Operação Lava Jato", *in Rev. Adm. Pública*, n° 2, Vol. 53, 2019, pp. 271-290, disponível em <URL:http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-76122019000200271&lng=en&nrm=iso>, consult. 18.01.2022.

Grupenmacher, Giovana Treiger, *As Plataformas de Negociação de Criptoativos: Uma análise comparativa com as atividades das corretoras e da Bolsa sob a perspectiva da proteção do investidor e da prevenção à lavagem dinheiro*, Dissertação (Mestrado em Direito), Escola de Direito da Fundação Getulio Vargas, São Paulo, 2019.

Guedes, Inês; Cruz, José Neves, "Infrações económicas e financeiras: aplicação da Teoria da Associação Diferencial de Sutherland", *In Infrações econômicas e financeiras: estudos de Criminologia e Direito,* AA.VV., Coimbra, Coimbra, 2013, pp. 88-101.

Harada, Kiyoshi, *Direito financeiro e tributário* [Em linha], 30ª ed., São Paulo, Atlas, 2021, disponível em <URL:https://integrada.minhabiblioteca.com.br/#/books/9786559770038/>, consult. 02.01.2022.

Iso, "ISO 22739:2020 Blockchain and distributed ledger technologies — Vocabulary" [Em linha], 2020, disponível em <URL:https://www.iso.org/standard/73771.html>, consult. 27.11.2021.

Jacob, Manuel Luís Moura, *A Tributação dos Criptoativos*, Dissertação (Mestrado em Direito), Universidade Católica Portuguesa, Porto, 2022.

Kobayashi, Eduardo Mesquita, "Regulação de criptoativos no Japão - Marco regulatório, jurisprudência e doutrina", *in Rev. de Direito Público da Economia – RDPE* [Em linha], n° 67, ano 17, 2019, Belo Horizonte, Fórum, pp. 115-136, disponível em <URL:https://www.researchgate.net/publication/338779262_Regulacao_de_criptoativos_no_Japao_-_Marco_regulatorio_jurisprudencia_e_doutrina_Cryptoassets_Regulation_in_Japan_-_Legal_framework_case_law_and_theory>, consult. 13.02.2022.

Kuchar; Natália, "Contratos digitais: status atual e novas fronteiras", *In Direito e Novas Tecnologias* [Em linha], Costa-Corrêa, André; Predolim, Emerson Alvarez; Longhi, Maria Isabel Carvalho Sica; Rebouças, Rodrigo Fernandes, São Paulo, Almedina Brasil, 2020, pp. 481-502, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 02.01.2022.

Kurtz, Lahis; Lorenzo, Florencia; Rodrigues, Gustavo, "A regulação da União Europeia sobre criptomoedas e riscos de lavagem de dinheiro: uma análise crítica da Quinta Diretiva Antilavagem de Dinheiro frente aos provedores de serviços de criptomoeda" [Em linha], Instituto de Referência em Internet e Sociedade, Belo Horizonte, 2020, disponível em <URL:https://bit.ly/3cQIHM5>, consult. 07.04.2022.

Laan, Cesar van der, É crível uma economia monetária baseada em bitcoins? *Limites à disseminação de moedas virtuais privadas* [Em linha], Brasília, Núcleo de Estudos e Pesquisas/CONLEG/Senado, 2014, disponível em <URL:https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td163>, consult. 06.01.2022.

Laurence, Tiana, *Blockchain Para Leigos* [Em linha], Rio de Janeiro, Alta Books, 2019, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9788550808024/>, consult. 27.11.2021.

Luz, Joana Alexandre Giraldes Vieira, *Regulação e Criptomoedas*, Dissertação (Mestrado em Direito), Universidade de Lisboa, Lisboa, 2020.

Lyons, Tom; Courcelas, Ludovic; Timsit, Ken, *Legal and regulatory framework of blockchains and smart contract* [Em linha], 2019, disponível em <URL:https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf>, consult. 10.06.2020.

Macedo, Adriana, *Tributação das criptomoedas: enquadramento fiscal dos rendimentos derivados das criptomoedas em sede de IRS*, Dissertação (Mestrado em Direito), Faculdade de Direito da Universidade do Porto, Porto, 2021.

Maia, Guilherme Campos, *O Enquadramento Jurídico-Fiscal dos Criptoativos em sede de IRS*, Dissertação (Mestrado em Direito), Universidade Católica Portuguesa, Porto, 2019.

Maia, Guilherme Campos; Santos, João Vieira dos, "MiCA and DeFi ("Proposal for a Regulation on Market in Crypto-assets" and "Decentralised Finance")", *in Rev. Eletrónica de Direito* [Em linha], n° 2, Vol. 28, 2022, disponível em <URL:https://cij.up.pt/pt/red/edicoes-anteriores/2022-nordm-2/mica-e-defi-ldquoproposta-de-regulamento-sobre-mercados-de-criptoativosrdquo-e-financas-descentralizadasrdquo/>, consult. 30.03.2023.

Majone, Giandomenico, "Do Estado Positivo ao Estado Regulador: causas e consequências da mudança no modo de governança", *In Regulação econômica e democracia: o debate europeu*, São Paulo, Singular, 2006.

Malaquias, Pedro Ferreira, "Criptoativos: uma realidade de hoje", *in Actualidad Jurídica Uría Menéndez* [Em linha], Vol. 56, 2021, pp. 29-70, disponível em <https://www.uria.com/documentos/publicaciones/7623/documento/art01.pdf?id=12517&forceDownload=true>, consult. 30.03.2023.

Maltez, Joana Veríssimo; Cruz, José Nevez, "A teoria da escolha racional e as infrações económicas e financeiras", *In Infrações econômicas e financeiras: estudos de Criminologia e Direito,* AA.VV., Coimbra, Coimbra, 2013, pp. 149-163.

Maragno, L. M. D.; Knupp, P. de S.; Borba, J. A, "Corrupção, lavagem de dinheiro e conluio no Brasil: evidências empíricas dos vínculos entre fraudadores e co-fraudadores no caso Lava Jato", *in Rev. de Contabilidade e Organizações*, Vol. 13, 2019, pp. 5-18, disponível em <URL:http://www.revistas.usp.br/rco/article/view/158510>, consult. 27.11.2021.

Medaglia, Thiago Rufalco; Visini, Eric Simões, "Breves considerações sobre o tratamento legal, contábil e fiscal das moedas virtuais". *In Tributação da economia digital: desafios no Brasil, experiência internacional e novas perspectivas* [Em linha], Monteiro, Alexandre Luiz Moraes do Rêgo; Faria, Renato Vilela; Silveira, Ricardo Maitto da,. São Paulo, Saraiva, 2018, pp. 625-641, disponível em <URLS:https://integrada.minhabiblioteca.com.br/#/books/9788553604500/>, consult. 02.01.2022.

Meira, Liziane Angelotti; Dall'ora, Fillipe Soares; Santana, Hadassah Laís S., **"**Tributação de novas tecnologias: o caso das criptomoedas" *In Tributação 4.0* [Em linha], Santana, Hadassah, L.; Afonso, José Roberto, São Paulo, Almedina Brasil, 2020, pp. 341-356, disponível em <URL:https://integrada.minhabiblioteca.com.br/#/books/9788584936274/>, consult. 02.01.2022.

Mendroni, Marcelo Bartlouni, *Crime de lavagem de dinheiro* [Em linha], 4ª ed. rev., atual. e ampl., São Paulo, Atlas, 2018, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9788597016796/>, consult. 23.12.2021.

Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System* [Em linha], 2008, disponível em <URL:https://bitcoin.org/bitcoin.pdf>, consult. 27.11.2021.

Neves; Barbara das; Cíceri; Pedro Vitor Botan, "Tributação dos criptoativos no Brasil: desafios das tecnologias disruptivas e o tratamento tributário brasileiro", *in Rev. Jurídica da Escola Superior de Advocacia da OAB-PR* [Em linha], n° 3, ano 3, 2018, pp. 125-163, disponível em <URLS:http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2018/12/revista_esa_8_07.pdf>, consult. 02.01.2022.

Neves, Marcelo, *Transconstitucionalismo***,** São Paulo, Martins Fontes, 2009.

Nunes, Marcelo Guedes, *Jurimetria: como a Estatística pode reinventar o Direito*, 2ª ed., São Paulo, Thomson Reuters Brasil, 2019, disponível em <URL:https://proview.thomsonreuters.com/library.html#/library>, consult. 18.01.2022.

Nunes, Leandro Bastos, "O Bitcoin-cabo na condição de meio para a consumação de crimes econômicos" [Em linha], Associação Nacional do Ministério Público, disponível em <ULR:https://www.anpr.org.br/imprensa/artigos/25690-o-bitcoin-cabo-na-condicao-de-meio-para-a-consumacao-de-crimes-economicos>, consult. 02.01.2022.

OECD, "OECD Blockchain Primer" [Em linha], 2018, disponível em <URL:https://www.oecd.org/finance/ OECD-Blockchain-Primer.pdf>, consult. 27.11.2021.

—, "The Sharing and Gig Economy: Effective Taxation of Platform Sellers: Forum on Tax Administration" [Em linha], Paris, OECD Publishing, 2019, disponível em <URL:https://doi.org/10.1787/574b61f8-en>, consult. 18.01.2022.

—, "Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues" [Em linha], OECD, Paris, 2020, disponível em <URL:https://www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.pdf>, consult. 05.04.2022.

—, "Regulatory Approaches to the Tokenisation of Assets" [Em linha], OECD Blockchain Policy Series, 2021, disponível em <URL:https://www.oecd.org/daf/fin/financial-markets/Regulatory-Approaches-to-the-Tokenisation-of-Assets.pdf>, consult. 05.04.2022.

—, "Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard" [Em linha], OECD, 2022, disponível em <URL:https://www.oecd.org/tax/exchange-of-tax-information/public-consultation-document-crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf>, consult. 05.04.2022.

—, "Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard" [Em linha], OECD, Paris, 2022, disponível em <URL:https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-tothe-common-reporting-standard.htm>, consult. 30.03.2023.

Paulino, Inês Valente, *As Criptomoedas: Desafios à Regulação*, Dissertação (Mestrado em Economia Internacional e Estudos Europeus), Universidade de Lisboa, Lisboa, 2019.

Pereira, Liliana; Ferreira, Juliana, "A Tributação do Rendimento Derivado das Transações com a Moeda Virtual "Bitcoin", *In LegalTech, Artificial Intelligence and the Future of Legal Practice*, Veiga, Fábio da Silva; Zalucki, Mariusz (coords.), Porto/Kraków, Instituto Iberoamericano de Estudos Jurídicos and AFM Kraków University, 2022, pp. 321-331.

Pinheiro, Reginaldo César, *Os cybercrimes na esfera jurídica brasileira* [Em linha], 2000, disponível em <URL:http://jus.com.br/revista/texto/1830>, consult. 10.06.2020.

Piscitelli, Tathiane, "Criptomoedas e os possíveis encaminhamentos tributários à luz da legislação nacional", *in Rev. Direito Tributário Atual* [Em linha], São Paulo, IBDT, n° 40, 2018, pp. 572-590, disponível em <URL:https://ibdt.org.br/RDTA/wp-content/uploads/2018/11/Tathiane-Piscitelli.pdf>, consult. 02.01.2022.

Portugal, Centro Nacional de Cibersegurança, "Relatório Cibersegurança em Portugal Riscos & Conflitos 2021" [Em linha], 2021, disponível em <URL:https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurancа-cncs.pdf>, consult. 23.12.2021.

Portugal, "Lei 58/2020, de 31 de agosto", D.R. I Série, 169 (2020-08-31), pp. 3–206, disponível em <URL:https://dre.pt/dre/detalhe/lei/58-2020-141382321>, consult. 16.07.2022.

—, "Lei 79/2021, de 24 de novembro". D.R. I Série, 228 (2021-11-24), pp. 9-38, disponível em <URL:https://files.dre.pt/1s/2021/11/22800/0000900038.pdf>, consult. 16.07.2022.

Prado, Luiz Regis, *Direito Penal Econômico* [Em linha], 9ª ed., Rio de Janeiro, Forense, 2021, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786559641192/>, consult. 23.12.2021.

PwC, "PwC Global Crypto Regulation Report 2023" [Em linha], PwC, 2022, disponível em <URL:https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/pwc-global-crypto-regulation-report-2023.pdf>, consult. 30.03.2023.

Rebouças, Rodrigo Fernandes, "Contratos eletrônicos: smart contracts"**,** *In Direito e Novas Tecnologias* [Em linha], Costa-Corrêa, André; Predolim, Emerson Alvarez; Longhi, Maria Isabel Carvalho Sica; Rebouças, Rodrigo Fernandes, São Paulo, Almedina Brasil, 2020, pp. 591 a 616, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 02.01.2022.

—, *Contratos Eletrônicos***,** 2ª ed., Almedina, São Paulo, 2018.

Revoredo, Tatiana, *Blockchain: tudo o que você precisa saber*, 1ª ed., Amazon, The Global Strategy, 2019.

Ribeiro, David Montezuma Mota, *Bitcoin e Direito Penal: uma breve análise da moeda virtual como meio para o crime de sonegação fiscal* [Em linha], Instituto Brasileiro de Direito Penal Econômico, 2021, disponível em <URL:https://ibdpe.com.br/bitcoin-e-direito-penal-uma-breve-analise-da-moeda-virtual-como-meio-para-o-crime-de-sonegacao-fiscal/>, consult. 02.01.2022.

Ribeiro, João Sérgio, *Direito Fiscal da União Europeia: tributação direta***,** Coimbra, Almedina, 2019.

Rizzo, Maria Balbina Martins de, *Prevenção da lavagem de dinheiro nas organizações* [Em linha], 2ª ed. atual. e rev., São Paulo, Trevisan, 2016, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9788599519875/>, consult. 23.12.2021.

Rolo, António Garcia, "A proposta de Regulamento europeu sobre mercados de criptoativos: breve sumário e análise", *in Rev. de Direito das Sociedades* [Em linha], ano XIII, n° 2, 2021, pp. 285-300, disponível em <http://www.revistadedireitodassociedades.pt/files/RDS%202021-02%20(285-300)%20-%20Breves%20coment%C3%A1rios%20-%20Ant%C3%B3nio%20Garcia%20Rolo%20-%20A%20proposta%20de%20Regulamento%20europeu%20sobre%20mercados%20de%20criptoativos%3A%20breve%20sum%C3%A1rio%20e%20an%C3%A1lise.pdf>, consult. 30.03.2023.

Ross, Alec, *As indústrias do futuro*, Coimbra, Conjuntura Actual Editora, 2016.

Santos, João Vieira dos, "Soft Law e boa governança no mercado das criptomoedas", *in Rev. Eletrônica de Direito* [Em linha], n° 2, Vol. 16, 2018, disponível em <URL:https://cije.up.pt/client/files/0000000001/9_589.pdf>, consult. 16.07.2022.

Schoueri, Luis. Eduardo, *Direito Tributário* [Em linha], São Paulo, Saraiva Educação, 2021, disponível em <URL:https://integrada.minhabiblioteca.com.br/#/books/9786555592696/>, consult. 02.01.2022.

—, "Tributação da renda oriunda do comércio eletrônico na esfera internacional: de volta à tributação pelo Estado da fonte", *In Direito e Novas Tecnologias* [Em linha], Costa-Corrêa, André; Predolim, Emerson Alvarez; Longhi, Maria Isabel Carvalho Sica; Rebouças, Rodrigo Fernandes, São Paulo, Almedina

Brasil, 2020, pp. 375 a 396, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 02.01.2022.

Silveira, Renato de Mello Jorge, "Criptocrime": considerações penais econômicas sobre criptomoedas e criptoativos", *in Rev. de Direito Penal Econômico e Compliance* [Em linha], Vol. 1, 2020, disponível em <URL:https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/white-paper/rdpec-1-renato-de-mello.pdf>, consult. 23.12.2021.

—, *Bitcoin e suas fronteiras penais: em busca do marco penal das criptomoedas*, Belo Horizonte, D' Plácido, 2018.

Steffens, Luana; Tessari, Claudio, "A tributação das operações com criptomoedas no Brasil: o caso da bitcoin", *in Rev. de Direito Tributário Contemporâneo* [Em linha], Vol. 30, 2021, pp. 269-296, disponível em <URL:http://tessaripohlmann.adv.br/wp-content/uploads/2021/09/artigo-39.pdf>, consult. 02.01.2022.

Szabo, Nick, *Smart Contracts: Building Blocks for Digital Markets* [Em linha], 1996, disponível em <URL:https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html>, consult. 02.01.2022.

Teixeira, Glória, *Manual de Direito Fiscal*, Coimbra, Almedina, 2019.

—, "Reforma do Sistema Fiscal – IRS", *In Uma Reforma Fiscal para o Século XXI* [Em linha], AA. VV., Partido Social Democrata, [S. l], [S. d.], pp. 45-54, disponível em <URL:https://www.psd.pt/pt/cen/reforma-fiscal-para-o-seculo-xxi>, consult. 18.07.2022.

Teixeira, Tarcisio, *Direito Digital e Processo Eletrônico* [Em linha], São Paulo, Saraiva Educação, 2020, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786555591484/>, consult. 27.11.2021.

Teixeira, Vanessa Jordana da Silva, *A tributação em sede de IVA de Moedas Virtuais no âmbito da União Europeia: o caso do Bitcoin*, Dissertação (Mestrado em Direito), Faculdade de Direito da Universidade do Porto, Porto, 2017.

Telles, Christiana Mariani da Silva, *Sistema Bitcoin, Lavagem de Dinheiro e Regulação*, Dissertação (Mestrado em Direito), Escola de Direito da Fundação Getúlio Vargas, Rio de Janeiro, 2018.

The Law Library of Congress, "Regulation of Criptocurrency around the world. Report. Global Legal Research Center" [Em linha], Nov. 2021, disponível em <URL:https://tile.loc.gov/storage-services/service/ll/llglrd/2021687419/2021687419.pdf>, consult. 26.01.2022.

Torres, Heleno Taveira, *Direito tributário e direito privado*, São Paulo, Revista dos Tribunais, 2003.

Uhdre, Dayana de Carvalho, *Blockchain, tokens e criptomoedas: análise jurídica*, São Paulo, Almedina, 2021.

Ulrich, Fernando, *Bitcoin: a moeda na era digital*, São Paulo, Instituto Ludwig von Mises Brasil, 2014.

Valadão, Marcos Aurélio P.; GASSEN, Valcir, *Tributação nos Estados Unidos e no Brasil* [Em linha], São Paulo, Almedina, 2020, disponível em <URL:https://integrada.minhabiblioteca.com.br/#/books/9788584936267/>, consult. 30.01.2022.

Venezuela, Governo Bolivariano, "Petro: Hacia la Revolución Digital Económica" [Em linha], Superintendencia Nacional de Criptoativos y Actividades Conexas, 2017, disponível em <URL:https://petro.gob.ve/static/images/petro-whitepaper.pdf>, consult. 30.01.2022.

Vita, Jonathan Barros, "Serviços virtuais e a localização da prestação do serviço: (re) analisando o conceito de estabelecimento tributário no direito brasileiro e internacional", *In Direito e Novas Tecnologias* [Em linha], Costa-Corrêa, André; Predolim, Emerson Alvarez; Longhi, Maria Isabel Carvalho Sica; Rebouças, Rodrigo Fernandes, São Paulo, Almedina Brasil, 2020, pp. 301 a 314, disponível em <URL:https://app.minhabiblioteca.com.br/#/books/9786556271101/>, consult. 02.01.2022.

Wellisch, Julya Sotto Mayor, *Mercado de Capitais: fundamentos e desafios*, São Paulo, Quartier Latin, 2018.

World Economic Forum, "The Global Competitiveness Report 2019" [Em linha], 2019, disponível em <URL:https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf >, consult. 11.02.2022.

—, "The Global Competitiveness Report Special Edition 2020" [Em linha], 2020, disponível em <URL:https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2020.pdf >, consult. 11.02.2022.

—, "Guidelines for Improving Blockchain's Environmental, Social and Economic Impact" [Em linha], disponível em <URL:https://www.weforum.org/reports/guidelines-for-improving-blockchain-s-environmental-social-and-economic-impact/>, consult. 15.04.2023.

Yazbek, Otavio, *Regulação do Mercado Financeiro e de Capitais*, Rio de Janeiro, Elsevier, 2007.

JURISPRUDÊNCIA CITADA

Brasil, Superior Tribunal de Justiça, *CC 161.123/SP* [Em Linha], Rel. Ministro Sebastião Reis Júnior, Terceira Seção, julgado em 28.11.2018, DJe 05.12.2018, disponível em <URL:https://scon.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=CC+161123&b=ACOR&p=false&l=10&i=5&operador=E&tipo_visualizacao=RESUMO>, consult. 28.02.2022.

—, *HC 530.563/RS* [Em linha], Rel. Ministro Sebastião Reis Júnior, Sexta Turma, julgado em 05.03.2020, DJe 12.03.2020, disponível em <URL:https://scon.stj.jus.br/SCON/pesquisar.jsp?newsession=yes&tipo_visualizacao=RESUMO&b=ACOR&livre=HC+530563>, consult. 28.02.2022.

União Europeia, Acórdão do Tribunal de Justiça da União Europeia (Quinta Secção) de 22 de outubro de 2015 [Em linha], *Skatteverket contra David Hedqvist* (Processo C-264/14), ECLI:EU:C:2015:718, disponível em <URL:https://curia.europa.eu/juris/liste.jsf?num=C-264/14>, consult. 02.01.2022.