CIJ
CENTRO DE INVESTIGAÇÃO INTERDISCIPLINAR EM JUSTIÇA

CIJ Research Papers
Cadernos de Investigação CIJ

6 | 2024

A REFORMA DA CIBERSEGURANÇA NA UNIÃO EUROPEIA. O REGIME JURÍDICO DE CIBERSEGURANÇA INSTITUÍDO PELA DIRETIVA (UE) 2022/2555. IMPACTO SOBRE O QUADRO NORMATIVO PORTUGUÊS

Graça Enes
Investigadora Integrada do CIJ | Professora Associada da FDUP
Augusto Batalha Monteiro
Mestrando em Ciências Jurídico-Políticas na FDUP
Flávia Oliveira
Mestranda em Ciências Jurídico-Políticas na FDUP

Ficha Técnica

Autor | Graça Enes | Augusto Batalha Monteiro | Flávia Oliveira
Título | A Reforma da Cibersegurança na União Europeia. O Regime Jurídico de Cibersegurança Instituído pela Diretiva (UE) 2022/2555. Impacto sobre o Quadro Normativo Português
Data de Publicação| Setembro 2024
ISSN | 2975-836X
DOI | 10.34626/9-2024/2975-836X

Edição

Centro de Investigação Interdisciplinar em Justiça (CIJ) / Centre for Interdisciplinary Research on Justice (CIJ)
Financiamento | Este trabalho foi desenvolvido com o apoio da Fundação para a Ciência e a Tecnologia (FCT) – UIDB/00443/2020 (Centro de Investigação Jurídica)

Comissão Editorial

Secretariado

Contactos

Telefone | 222 041 610
Email | cij@direito.up.pt
Morada | Faculdade de Direito da Universidade do Porto
Rua dos Bragas, 223
4050-123, Porto
Portugal

A REFORMA DA CIBERSEGURANÇA NA UNIÃO EUROPEIA. O REGIME JURÍDICO DE CIBERSEGURANÇA INSTITUÍDO PELA DIRETIVA (UE) 2022/2555. IMPACTO SOBRE O QUADRO NORMATIVO PORTUGUÊS

Graça Enes

Investigadora Integrada e Diretora do CIJ. Professora Associada da FDUP. Titular do Módulo Jean Monnet DigEUCit "A Digital Europe for Citizens. Constitutional and Policymaking Challenges".

Augusto Batalha Monteiro

Mestrando em Ciências Jurídico-Políticas na FDUP.

Flávia Oliveira

Mestranda em Ciências Jurídico-Políticas na FDUP

(Quaisquer questões relacionadas com o conteúdo do presente artigo deverão ser dirigidas aos autores, através do seguinte endereço de email: gferreira@direito.up.pt)

Resumo

O presente estudo pretende descrever, em geral, o panorama da cibersegurança na UE e em Portugal e a analisar, em especial, o regime jurídico instituído pela Diretiva (UE) 2022/2555, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança no âmbito da União Europeia, e os impactos deste novo regime jurídico na legislação portuguesa, em especial as eventuais alterações legislativas necessárias para a adaptação do quadro normativo nacional à referida diretiva.

Abstract

This study aims to describe, in general, the cybersecurity landscape in the EU and Portugal and to analyse, in particular, the legal regime established by Directive (EU) 2022/2555, concerning measures to ensure a high common level of cybersecurity within the European Union, and the impacts of this new legal regime on Portuguese legislation, in particular any legislative changes necessary to adapt the national regulatory framework to the aforementioned directive.

Índice

INTRODUÇÃO

No presente, é nítida a importância da tecnologia e do meio digital na vida e no funcionamento da sociedade. O mundo real e a vida das pessoas estão progressivamente imbricados com o mundo digital, o que se vê mesmo em atividades cotidianas das mais singelas, como o uso de serviços de transporte urbano, a aquisição de produtos de mercado, a realização de transações bancárias, o exercício de atividades profissionais em *home office*, a utilização de redes sociais, dentre tantas outras. As atividades das empresas, das organizações e dos Estados são absolutamente dependentes da tecnologia e do meio digital, tanto na sua organização interna como nos seus processos comunicacionais. Em suma, o espaço físico prolonga-se no ciberespaço.

A acelerada transição digital em todos os domínios e o crescimento exponencial da prestação de serviços online, incluindo de serviços públicos, incontornável desde a pandemia COVID-19, tornam crucial a cibersegurança, pois esta evolução não sucede sem riscos também crescentes. Prevê-se que, em 2025, o mundo contará com 25 biliões de dispositivos conectados, ¼ dos quais na Europa. Mais de 50% da população do mundo acede à "www" e o número cresce diariamente com um milhão de novos utilizadores[1]. Já os ciberataques têm aumentado e são cada vez mais sofisticados[2].

A Estratégia de Cibersegurança Europeia, apresentada pela Comissão Europeia e pelo Alto Representanto para os Negócios Estrangeiros e Política de Segurança em dezembro de 2020 [COM (2020)18 final], prevê três instrumentos principais para implementar a política de cibersegurança europeia: o instrumento regulatório; o investimento; e, a ação política, incluindo diplomática. Será a reforma do primeiro instrumento, empreendida em dezembro de 2022 pela Diretiva (UE) 2022/2555 (também designada de Diretiva "SRI 2"), que será o foco da análise que se segue. A abordagem será analítico-descritiva. Depois de um breve excurso sobre o ciberespaço, a cibersegurança e as principais exigências da normatividade, na União Europeia e em Portugal, será apresentada uma panorâmica do quadro institucional de governação da cibersegurança na União Europeia e em Portugal, avançando-se depois para a análise da evolução do regime entre a anterior Diretiva "SRI 1" e a Diretiva "SRI 2".

1. O CIBERESPAÇO, A CIBERSEGURANÇA, O DIREITO E OS DIREITOS

O ciberespaço é um conceito objeto de tantas definições quantos os seus autores, havendo apenas acordo sobre a sua natureza dinâmica e crescentemente ubíqua[3]. A impossibilidade de uma definição única de ciberespaço comprova-se pelas diversas

[1] RAMOS, Maria Elisabete. (2021) "Corporate governance and cyber governance. How to govern the future?", E.TEC Yearbook. Governance & Technology, UMinho, Braga, p. 157 – p. 178, p. 159.
[2] Proposta de Diretiva SRI 2 [COM(2020) 823 final], p. 1.
[3] Para uma síntese desse conceito, veja-se Barbosa Caseiro, I. (2022). "A Segurança do Ciberespaço europeu" https://eurodefense.pt/wp-content/uploads/2022/11/02_A-Seguran%C3%A7a-do-Ciberespa%C3%A7o-Europeu-13OUT2021.pdf , [último acesso em 23.03.2023]. Para maiores desenvolvimentos, Santos, L., Marques Guedes, A. (2015). Breves reflexões sobre Poder e Ciberespaço, RDeS – Revista de Direito e Segurança, n.° 6 (julho / dezembro de 2015): 189-209; Lance Strate (1999) The varieties of cyberspace: Problems in definition and delimitation, Western Journal of Communication, 63:3, 382-412, DOI: 10.1080/10570319909374648.

definições presentes nessa entrada do Glossário do NIST[4]. A Estratégia Nacional de Segurança do Ciberespaço (ENSC) apresenta a seguinte definição: "[o] ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação". No presente, o ciberespaço é um espaço de exercício de poder, no sentido proposto por Foucault de "poder do discurso"[5], seja como via para a persuasão, para a marcação da agenda política ou mediática, seja como via para a manipulação da perceção dos utilizadores. A relevância do ciberespaço comprova-se no seu reconhecimento como o quinto domínio operacional de exercício da soberania (terra, mar, água, espaço e ciberespaço)[6].

Se o mundo real e o mundo virtual se desenvolvem em simbiose, a proteção dos direitos fundamentais e a salvaguarda do Direito não podem ser menosprezados em nenhum deles[7]. Na sociedade em rede, os riscos e as ameaças são ubíquos e permanentes. Os custos pessoais, patrimoniais e até existenciais dos incidentes para os indivíduos, empresas, organizações sociais e Estados são, independentemente da origem e da sua natureza, elevadíssimos e quase incontáveis, dadas as significativas cifras negras. Os incidentes de segurança no ciberespaço possuem um elevado potencial de lesão aos direitos fundamentais, nomeadamente relacionado com a privacidade, a propriedade, a liberdade, a saúde e até a vida. Basta lembrar a violação recorrente de dados pessoais e os múltiplos usos criminosos possíveis para esses dados. As ameaças são múltiplas e diversas; além da criminalidade comum, as tensões geopolíticas e as ações híbridas têm aumentado[8]. A Diretiva 2022/2555 reconhece o aumento das ameaças, em especial o aumento exponencial de *ransomware*[9]. A generalização da utilização do espaço digital entre as PME acarreta novos desafios de segurança, dadas as dificuldades e necessidades específicas[10], tal como salienta também a mesma Diretiva. No entanto, ainda se verifica um baixo nível de resiliência cibernética das empresas que operam na UE e diferentes níveis de consistência, no que se refere à resiliência entre Estados Membros, o que provoca dificuldades, perante uma realidade que exige uma capacidade de resposta conjunta. Em 2020, 42% dos europeus não dispunha de competências digitais básicas. Esta realidade impõe elevadas exigências ao ecossistema de cibersegurança.

A cibersegurança é um conceito complexo[11]. De um modo sumário, visa assegurar a disponibilidade e integridade das redes e infraestruturas digitais e a confidencialidade da informação nelas contida. A Estratégia Nacional de Segurança no Ciberespaço descreve-a como "o conjunto de medidas e ações de prevenção, monitorização, deteção, reação,

[4] https://csrc.nist.gov/glossary/term/cyberspace [último acesso em 23.02.2024].
[5] Foucault, M. (1997). A Ordem do Discurso, trad. port., Lisboa, Relógio de Água.
[6] Em 2018, a UE classificou o ciberespaço como um domínio da atividade militar.
[7] Tal foi sublinhado na "Paris Call for Trust and Security in Cyberspace", de 11.12.2018, apoiada por Estados, regiões, municípios, empresas, reguladores e outras organizações da sociedade civil, e onde se inscreveram "9 princípios", disponível em https://pariscall.international/en/principles [último acesso em 26.03.2023]
[8] A Estratégia Europeia para a Cibersegurança fala de um "cenário de ameaças complexo". Comissão Europeia e Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança (2020). Comunicação Conjunta ao Parlamento Europeu e ao Conselho "Estratégia de cibersegurança da UE para a década digital" [JOIN (2020)18 final], 1-4.
[9] Considerandos n.ºs 54, 56 e 6 e artigo 14º, nº 4, s). Em virtude do seu impacto, este é considerado um risco sistémico. Pernik, P. (2022), "Drivers of Change Impacting Cyberspace in 2030", in Piret Pernik (ed.), *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, 56-79, 59, disponível em https://ccdcoe.org/uploads/2022/03/Horizon_Scanning_v2_170x240_220513.pdf [último acesso em 26.03.2023]
[10] Segundo o Eurobarómetro, 48% das PMEs portuguesas admitiram, em 2021, ter sofrido pelo menos um cibercrime nos últimos 12 meses, enquanto a média da UE foi de 21%, disponível em https://europa.eu/eurobarometer/surveys/detail/2280 [último acesso em 26.03.2024].
[11] Para uma panorâmica dessa complexidade, vide Štrucl, D. (2021). Comparative study on the cyber defence of NATO Member States, NATO Cooperative Cuber Defence Centre of Excellence, disponível em https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf [último acesso em 26.03.2023]

análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem". Numa perspetiva lata, a missão da cibersegurança é assegurar a dissuasão e reconstituição, através da resiliência, e a prevenção e repressão, através da identificação dos infratores e posterior punição[12]. Segundo o Regulamento 2019/881, relativo à ENISA e à certificação da cibersegurança das tecnologias da informação e comunicação, abrange todas as atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas[13]. A Diretiva 2022/2555, no seu artigo 6.º, ponto 3) remete para essa definição. A maior abrangência e precisão do elenco de definições desta diretiva comprova um alcance abrangente, dissuasor, preventivo, corretivo e mitigador. Em especial, os eventos relevantes, independentemente da sua causa ou condições da ocorrência, incluem os "quase incidentes", os "incidentes" e os "incidentes de cibersegurança em larga escala".

A cibersegurança tem assumido uma relevância progressivamente transversal, sendo notória uma evolução holística. Dada a digitalização da economia e da sociedade, a cibersegurança é uma necessidade que se impõe nos diversos domínios económicos e sociais, que se deve refletir na respetiva regulação e na ação das autoridades competentes. Na atualidade, a cibersegurança deve ser encarada como uma verdadeira política pública com um alcance transversal. As preocupações da União Europeia com a cibersegurança, por exemplo, estiveram presentes na regulação de matérias como o tratamento de dados pessoais (Diretivas 1995/46/CE e 1997/66/CE, e Regulamento UE 2016/679) ou o comércio eletrónico (Diretiva 2000/31/CE). A preocupação setorial com acibersegurança foi objeto das "Recommended practices to enhance cybersecurity in transport organisations" e do "Transport Cybersecurity Toolkit"[14].Esta realidade comprova que, seja na avaliação dos riscos e dos problemas, seja no recorte das soluções, a abordagem multidisciplinar é uma mais-valia[15].

É visível igualmente uma evolução securitária[16]. Mais do que um problema técnico ou de segurança privado ou público, tem uma projeção na segurança nacional e até na defesa, dimensões que têm adquirido crescente importância. A abordagem regulatória e de supervisão e controlo tem de refletir esta evolução. Já foi proposta a adoção de uma "Declaração Global sobre os Direitos e Responsabilidades dos Estados pela Cibersegurança" [17]. Apesar de múltiplas iniciativas, das quais a mais conhecida é a

[12] A definição do NIST é a seguinte: "*Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation*". https://csrc.nist.gov/glossary/term/cybersecurity, [último acesso em 23.03.2023].

[13] Por sua vez, as ciberameaças são "uma circunstância, um evento ou uma ação potenciais suscetíveis de lesar, perturbar ou ter qualquer outro efeito negativo sobre as redes e os sistemas de informação, os seus utilizadores e outras pessoas" (artigo 2.º, ponto 8).

[14]https://transport.ec.europa.eu/system/files/2020-12/cybersecurity-awareness-poster.pdf; https://transport.ec.europa.eu/system/files/2020-12/cybersecurity-toolkit_en.pdf.

[15] Um bom exemplo de uma análise multidisciplinar e transversal é o projeto conjunto do Massachussets Institute of Technology e da Universidade de Harvard, *Explorations in Cyber International Relations*, 2015, desenvolvido no âmbito do Minerva Program do Defense Department norte-americano, que envolveu investigadores das áreas da Engenharia, da Informática, do Direito, da Economia e da Ciência Política. Choucri, N. (prep.) (2015). *Explorations in Cyber International Relations. A Research Collaboration of MIT and Harvard University. The Final Report Version 1.2.* Cambridge: Mass., disponível em https://ecir.mit.edu/final-report [último acesso em 26.03.23].

[16] Sliwinski, K.F. (2014). Moving beyond the European Union's Weakness as a Cyber-Security Agent, Contemporary Security Policy, DOI: 10. 1080/ 13523260. 2014. 959261.

[17] Pernice, I. (2017). "Cybersecurity Governance. Making Cyberspace a Safer Place", HIIG Discussion Paper Series. Discussion Paper No. 2017-05, August 2017, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=30121 [último acesso em 26.03.2023].

Convenção de Budapeste sobre o cibercrime, o panorama jurídico internacional revela numerosas "zonas cinzentas" que favorecem ações lesivas no ciberespaço[18]. As Conclusões do Conselho de novembro de 2017 sobre as questões do ciberespaço reconheceram os crescentes vínculos entre cibersegurança e ciberdefesa e apelaram à intensificação da cooperação em matéria de ciberdefesa, incentivando nomeadamente a cooperação entre as comunidades civis e militares na resposta a incidentes. Salientaram também que um ciberincidente ou uma cibercrise particularmente graves poderiam constituir razão suficiente para um Estado Membro invocar a cláusula de solidariedade (artigo 222.º do TFUE) e/ou a cláusula de assistência mútua da UE (artigo 42.º, n.º 7 do TUE). Em 2019, o Conselho adotou a Decisão (PESC) 2019/797 e o Regulamento (UE) 2019/796, relativos a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros. Desde 2017 que a UE utiliza instrumentos de "ciberdiplomacia"[19] destinados a prevenir, desincentivar, dissuadir e responder a ciberatividades maliciosas. A "Estratégia de Cibersegurança Europeia para a Década Digital", apresentada em 16.12.2020, é uma Comunicação conjunta da Comissão Europeia e do Alto Representante para os Negócios Estrangeiros e Política de Segurança [JOIN (2020)18 final]. Em 10 de novembro de 2022, foi apresentada a Comunicação conjunta da Comissão e do Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança "Política de Ciberdefesa da UE", JOIN(2022) 49 final.

Se não parece possível, nem desejável, que haja um retrocesso quanto à presença da tecnologia e do meio digital na sociedade contemporânea, há um único caminho possível: o desenvolvimento em cibersegurança.

É imperativo que os esforços em cibersegurança estejam norteados pela proteção de direitos fundamentais[20] e pelo respeito por valores, como segurança, liberdade, solidariedade e inclusão[21]. Esses, que são os valores fundamentais dos nossos sistemas jurídicos, têm de presidir ao recorte da ação política e regulatória, em ordem a preservar o modelo social europeu e promover uma sociedade digital confiável, acessível, aberta e equitativa, ordenada segundo o Direito e respeitadora dos direitos[22].

A Comunicação "Década Digital" [COM (2021)118 final] recorda que todos os direitos fundamentais vigentes na ordem jurídica da União valem no espaço digital, embora enuncie alguns que são mais diretamente atinentes: "Liberdade de expressão, incluindo o acesso a informação diversificada, fiável e transparente; Liberdade de estabelecimento e exercício de uma atividade empresarial em linha; Proteção dos dados pessoais e da privacidade e direito a ser esquecido; Proteção da criação intelectual das pessoas no espaço em linha". São igualmente enunciados um conjunto de princípios ordenadores do ambiente em linha: "Acesso universal aos serviços de Internet; Um ambiente em linha seguro e de confiança; Educação e competências digitais universais para que as pessoas participem ativamente na sociedade e nos processos democráticos; Acesso a sistemas e

[18] Schmitt, M.N. (2017). "Grey Zones in the International Law of Cyberspace", The Yale Journal of International Law [Vol. 42: 2 2017], 1-21, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3180687# [ultimo acesso em 26.03.2023]
[19] https://www.consilium.europa.eu/pt/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/ [último acesso em 26.03.2024].
[20] No ponto, vale a referência às conhecidas dimensões subjetiva e objetiva dos direitos fundamentais.
[21] Leia-se a Declaração Europeia sobre os direitos e princípios digitais para a década digital, de 26 de janeiro de 2022, do Parlamento Europeu, do Conselho e da Comissão Europeia.
[22] Enes, G. (2021) "A União Europeia Digital. Uma governação multinível ao serviço das pessoas", E.TEC Yearbook. Governance & Technology, UMinho, Braga, 115-138, p. 119, disponível em https://repositorium.sdum.uminho.pt/bitstream/1822/79681/1/e_tek_yearbook_2021_web.pdf [último acesso em 23.02.2024].

dispositivos digitais que respeitem o ambiente; Administração e serviços públicos digitais acessíveis e centrados no ser humano; Princípios éticos para os algoritmos centrados no ser humano; Proteção e capacitação das crianças no espaço em linha; Acesso a serviços de saúde digitais."

A velocidade e a complexidade das inovações tecnológicas criam dificuldades ao estabelecimento de uma regulação jurídica em moldes tradicionais; as soluções legislativas correm o risco de se tornarem obsoletas muito rapidamente, a que acresce a dificuldade do operador do Direito em lidar com assuntos cujo conhecimento técnico ordinariamente não possui. A par disso, o setor digital e a cibersegurança possuem um inerente caráter transfronteiriço, as ameaças e riscos não conhecem fronteiras, o que reclama a atuação cooperativa de diversas autoridades competentes em múltiplas áreas e ao nível nacional e supranacional.

Nessa linha, assistiu-se a uma abordagem flexível, em que a autorregulação é acompanhada por recomendações – *v.g.* a Recomendação (EU) 2017/1584 da Comissão, de 13 de setembro de 2017, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala - e compromissos da pluralidade de stakeholders do setor (Estados e Organizações Internacionais, empresas, academia)[23], em vez da tradicional regulação de tipo legislativo, conduzindo, num primeiro momento, à perda de protagonismo dos Estados[24]. Uma das iniciativas paradigmáticas é constituída pelos Manuais de Tallin[25] elaborados no âmbito da NATO. Por sua vez, os principais operadores do setor elaboram os seus próprios quadros[26].

Já os organismos de estandardização são chamados a exercer a função de regulador no espaço digital, como sucede, aliás, nos restantes domínios tecnológicos, em articulação com agências regulatórias técnicas. Se esta abordagem é adequada e eficaz não elimina todos as dificuldades e problemas. Existem múltiplas entidades que definem standards e recomendações, quer globais - a Organização Internacional de Normalização (ISO), a Comissão Eletrotécnica Internacional (CEI), a União Internacional das Comunicações (ITU) -, regionais - o Instituto Europeu de Normalização das Telecomunicações (ETSI), o Comité Europeu de Normalização (CEN) e o Comité Europeu de Normalização Eletrotécnica (Cenelec) -, nacionais – v.g. o Instituto Português da Qualidade e o alemão Deutsches Institut für Normung e.V. (DIN), e até profissionais - o Internet Engineering Task Force (IETF), o 3rd Generation Partnership Project (3GPP) e o Institute of Electrical and Electronics Engineers (IEEE). Esta realidade comprova a consciência e procupação generalizadas, mas acarreta uma fragmentação horizontal e vertical e induz a confusão para os usuários. O diálogo entre todas essas entidades nem sempre é efetivo. A governação e regulação não acompanham o desenvolvimento tecnológico[27]. A UE está a preparar um quadro comum para a certificação[28]. Esta realidade não pode prescindir de

[23] OSULA, A-M & RÕIGAS, H. (eds.) (2016), International Cyber Norms: Legal, Policy & Industry Perspectives, Tallinn, NATO Publications, 15-16.
[24] MACÁK, K. (2016), "Is the international law of cybersecurity in crisis?", in N. Pissanidis et al. (eds.), Cyber Power: 2016 8th International Conference on Cyber Conflict, Tallinn, NATO Publications, pp. 127-139, 134-136; EGGENSCHWILER, J. (2019), International Cybersecurity Norm Development: The Roles of States Post-2017, EU Cyber Direct, 4-7.
[25]https://www.cambridge.org/pt/universitypress/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition?format=PB [último acesso em 23.02.2024].
[26] Nicholas, P., Ciglic, K. (2017). *Building an effective national cybersecurity agency*, Microsoft, disponível em https://www.microsoft.com/en-us/cybersecurity/content-hub/cybersecurity-agency-whitepaper [último acesso em 26.03.2024].
[27] Enes, G. (2021) "A União Europeia Digital. Uma governação multinível ao serviço das pessoas", E.TEC Yearbook. Governance & Technology, UMinho, Braga, 115-138, 122).
[28] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework [último acesso em 23.02.2024].

instrumentos jurídicos vinculativos, onde se plasmem os princípios, as regras e as competências das autoridades competentes pela supervisão, incluindo obviamente o regime sancionatório; uma regulação jurídica vinculante da cibersegurança é, certamente, necessária, ainda que deva efetivar-se sob os novos modelos de governação flexível do "New Legislative Framework"[29] e da "New Approach Harmonisation"[30]. Na cibersegurança, esse foi o caminho trilhado na UE desde 2016.

Não menos importantes são a educação e a sensibilização da sociedade no sentido de desenvolvimento de competências neste domínio. A ENISA tem entre as respetivas missões o apoio à coordenação e troca de boas práticas em matéria de educação[31]. Um dos objetivos da "Bússola Digital" para 2030 é assegurar que 80% dos adultos europeus tenham competências digitais básicas e que a UE conte com 20 milhões de especialistas em tecnologiais da Informação (TI). Em 18 de abril de 2023, a Comissão Europeia lançou a Cybersecurity Skills Academy. Em outubro de cada ano, a Comissão e a ENISA promovem o "Mês da Cibersegurança Europeia" (ECSM)[32].

Sem prejuízo da importância destas iniciativas, a educação, seja geral ou especializada, é uma competência dos EM, que têm a responsabilidade principal aliada ao apoio e coordenação das entidades europeias[33]. Um dos eixos de intervenção da Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019-2023, aprovada em 23 de maio de 2019, pela Resolução do Conselho de Ministros nº 92/2019, em Portugal, é justamente a prevenção, educação e sensibilização da sociedade para o uso seguro e responsável das tecnologias digitais[34].

2. QUADRO NORMATIVO E INSTITUCIONAL EUROPEU E PORTUGUÊS DA CIBERSEGURANÇA

A complexidade inerente ao ciberespaço e à cibersegurança conduziu ao desenvolvimento de uma governação institucional plural e multinível, um autêntico ecossistema com numerosos atores e responsabilidades diversas, mas igualmente com redundâncias e dependências recíprocas. Impõe-se uma regulação e um quadro institucional de governação multinível[35] que alcance um ponto de equilíbrio entre flexibilidade, para

[29] https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en [último acesso em 26.03.2024].
[30] https://eur-lex.europa.eu/EN/legal-content/summary/a-new-approach-to-technical-harmonisation.html [último acesso em 26.03.2024].
[31] Veja-se o documento "National Capabilities Assessment Framework", publicado em 2020, o documento "Raising Awereness of Cybersecurity. A key element of national cybersecurity strategies", publicado em 2021, e o mais recente "Developing National Vulnerability Programmes", de 2023.
[32]https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/european-cyber-security-month [último acesso em 26.03.2024].
[33] Sobre as ações nacionais, veja-se ENISA (2022). Cybersecurity Education Initiatives in the EU Member States, disponível em https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states[último acesso em 23.02.2024].
[34] A ENSC 2019-2023 foi aprovada a 23 de maio de 2019 pela Resolução do Conselho de Ministros nº 92/2019, em revisão da primeira estratégia adotada em 2015. Desenvolvida para responder à constante evolução digital, a ENSC 2019-2023 propõe-se apresentaruma abordagem compreensiva das necessidades de segurança do ciberespaço a nível nacional, com vista a proteger e defender as infraestruturas críticas, os serviços de informação, as entidades públicas e privadas, e os cidadãos, focando dimensões como a prevenção, a educação e sensibilização, o combate ao cibercrime, a investigação e o desenvolvimento, e ainda a cooperação nacional e internacional. Disponível em https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/92-2019-122498962 [último acesso em 23.02.2024].
[35] Como escreve G. Enes (2021), "a governação em rede do espaço digital é um truísmo. Uma realidade que funciona em rede tem de ser governada e regulada em rede ("A União Europeia Digital. Uma governação multinível ao serviço das pessoas", E.TEC Yearbook. Governance & Technology, UMinho, Braga, 115-138, 138).

atender à velocidade das transformações digitais, e a segurança jurídica de uma regulação vinculante; que seja capaz de articular-se com os instrumentos de *soft law*, com destaque para os organismos de estandardização; que seja transversal a domínios conexos; que reconheça a multiplicidade das causas dos incidentes, sejam falhas do sistema, eventos naturais, erros ou ações maliciosas de atores humanos ou organizações, tal como presente no Sistema de Gestão de Segurança da Informação das normas ISO/IEC 27000; que reconheça seu caráter transfronteiriço, como é típico do meio digital; que promova a cooperação entre as autoridades competentes; e que fomente a inclusão, a educação e a sensibilização da sociedade para uma condução segura e responsável de seus comportamentos no meio digital[36]. Em Portugal, o quadro normativo compreende múltiplos atos jurídicos. O primeiro é a Lei n.º 46/2018, de 12 de agosto, que estabelece o regime jurídico da segurança no ciberespaço e que transpõe a Diretiva (UE) 2016/1148, do PE e do Conselho de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevedo nível comum de segurança das redes e da informação em toda a União. Este ato foi complementado pelo Decreto-Lei n.º 65/2021, de 30 de julho, que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do PE e do Conselho, de 17 de abril de 2019. Já o Regulamento n.º 183/2022 configura a instrução técnica relativa a comunicações entre as entidades e o Centro Nacional de Cibersegurança.

Este quadro normativo fundamental foi operacionalizado numa primeira linha estruturante através do instrumento programático quadrianual "Estratégia Nacional de Segurança do Ciberespaço" (ENSC) 2019-2023, aprovada em Conselho de Ministros pela Resolução n.º 92/2019, de 23 de maio. Em linha com a Estratégia Europeia, os objetivos estratégicos assumidos passam por "maximizar a resiliência, promover a inovação e gerar e garantir recursos". Os doze objetivos fundamentais são desenvolvidos através de seis eixos de intervenção[37]. Cabe ao Plano de Ação anual a respetiva concretização.

Acompanhando a perspetiva holística referida, a ENSC prevê a articulação com a Estratégia Nacional de Combate ao Terrorismo, aprovada pela Resolução do Conselho de Ministros n.º 40/2023, de 3 de maio, a Estratégia para a Transformação Digital da Administração Pública 2021-2026 e o Respetivo Plano de Ação Transversal para a legislatura, aprovados pela Resolução do Conselho de Ministros 131/2021, de 26 de agosto, e, bem assim, com a Estratégia de Inovação tecnológica e Empresarial para Portugal 2018-2030, aprovada pela Resolução do Conselho de Ministros 25/2018, de 15 de fevereiro, e a Estratégia Nacional de Ciberdefesa, aprovada pela Resolução do Conselho de Ministros n.º 106/2022, de 2 de novembro.

Outros instrumentos são relevantes, tais como o Decreto-Lei n.º 81/2016, de 28 de novembro, que cria a Unidade Nacional de Combate ao Cibercrime e à Cibercriminalidade Tecnológica, o Decreto-Lei n.º 43/2020, de 21 de julho, que estabelece o Sistema Nacional de Planeamento Civil de Emergência, e o Decreto-Lei n.º 20/2022, de 28 de janeiro, que aprova os procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas críticas nacionais e europeias. São ainda relevantes a Lei n.º 16/2022, de 16 de agosto, que aprova a Lei das Comunicações Eletrónicas, e o Regulamento n.º 303/2019, de 1 de abril, da Autoridade Nacional de Comunicações

[36] ENISA, "Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies", February 2023, disponível em https://www.enisa.europa.eu/publications/building-effective-governance-frameworks-for-the-implementation-of-national-cybersecurity-strategies [último acesso em 23.02.2024].
[37] www.cncs.gov.pt/pt/estratégia-nacional/ [último acesso em 23.02.2024].

relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas. Finalmente, o Decreto-Lei n.º 3/2012, de 16 de janeiro, estabelece o quadro orgânico do Gabinete Nacional de Segurança, e o Despacho n.º 1195/2018 aprova o Regulamento Interno do Conselho Superior de Segurança do Ciberespaço.

O quadro normativo português não pode ser compreendido isoladamente, antes há que considerar outras fontes internacionais. Entre os quadros de referência da OCDE são exemplo as Recomendações aprovadas na Reunião Ministerial sobre Economia Digital, de 14 de novembro de 2022. Já o Conselho da Europa foi a fonte da primeira convenção internacional dirigida ao combate à cibercriminalidade – a Convenção de Budapeste - e continua a ser um espaço de cooperação relevante. Considerando a realidade geopolítica que se vive atualmente no território europeu, em que o domínio cibernético é uma das frentes de batalha do confronto, ilustração da desmaterialização do espaço estratégico, e uma das dimensões da soberania, ganham importância crescente documentos como os que a NATO vem dedicando ao tema, em especial o Tallin Manual 2.0, de 2017 (está em preparação o 3.0).

O quadro jurídico da União Europeia constitui o quadro de referência mais importante e constitui a base da legislação portuguesa. Se a Diretiva "SRI 1" foi adotada na sequência da Estratégia Europeia de Cibersegurança de 2013, uma nova Estratégia foi aprovada em 2020, marcando o início de um novo ciclo, cujo desenvolvimento já se tinha iniciado em 2019. Neste ano foi adotado o Regulamento 2019/881, relativo à ENISA e à certificação da cibersegurança das tecnologias da informação, que introduziu um quadro europeu para a certificação da cibersegurança de produtos, processos e serviços, além de conferir um mandato permanente à referida agência. Também em 2019 foi aprovada a Decisão (PESC) 2019/797 do Conselho, de 17 de maio, relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus EM, e o Regulamento (UE) 2019/1020 (Cyber Resilience Act).

A Estratégia europeia de 2020 ["Estratégia de cibersegurança da EU para a década digital", JOIN(2020) 18 final] é paradigmática da evolução registada, pois é uma Comunicação da Comissão Europeia e do Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança. Se, por um lado, aponta a insuficiência do quadro então vigente, salienta, por outro lado, a articulação com outras iniciativas transversais e setoriais, como a "Estratégia Digital Europeia", a "Estratégia da UE para a União da Segurança 2020-2025" ou a "Estratégia Ghlobal para a Política Externa e de Segurança da UE". Em geral, propõe-se o alargamento do âmbito subjetivo, a precisão dos setores envolvidos e o reforço do regime de supervisão e do regime sancionatório, com um reforço da institutionalização e uma procedimentalização acrescida.

Esta nova orientação político-legislativa tem sido desenvolvida através de instrumentos se soft law, de hard law e dos concomitantes recursos institucionais. Entre os primeiros, encontram-se os seguintes: a Recomendação (UE) 2021/1086 da Comissão, relativa à criação de uma Ciberunidade Conjunta, de 23.6.2021 [C(2021) 4520 final]; as Conclusões do Conselho sobre a estratégia para a cibersegurança para a década digital, de 9.3.2021; e a Recomendação do Conselho relativa a uma abordagem coordenada da União para reforçar a resiliência das infraestruturas críticas, de 8.12.2022 (2023/C20/01). Entre os segundos, além da Diretiva (UE) 2022/2555 relativa a medidas destinadas a garantir um elevados nível comum de cibersegurança na União (Diretiva "SRI 2"), elencam-se os seguintes: a Diretiva (UE) 2022/2556 relativa à resiliência operacional digital para o setor financeiro; a Diretiva (UE) 2022/2557 relativa à resiliência das entidades críticas (CER); e,

o Regulamento (UE) 2022/2554 relativo à resiliência operacional digital do setor financeiro (DORA). Ainda em fase de adoção encontra-se a Proposta de Regulamento relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais [COM(2022) 454 final] e que altera o Cyber Resilience Act.

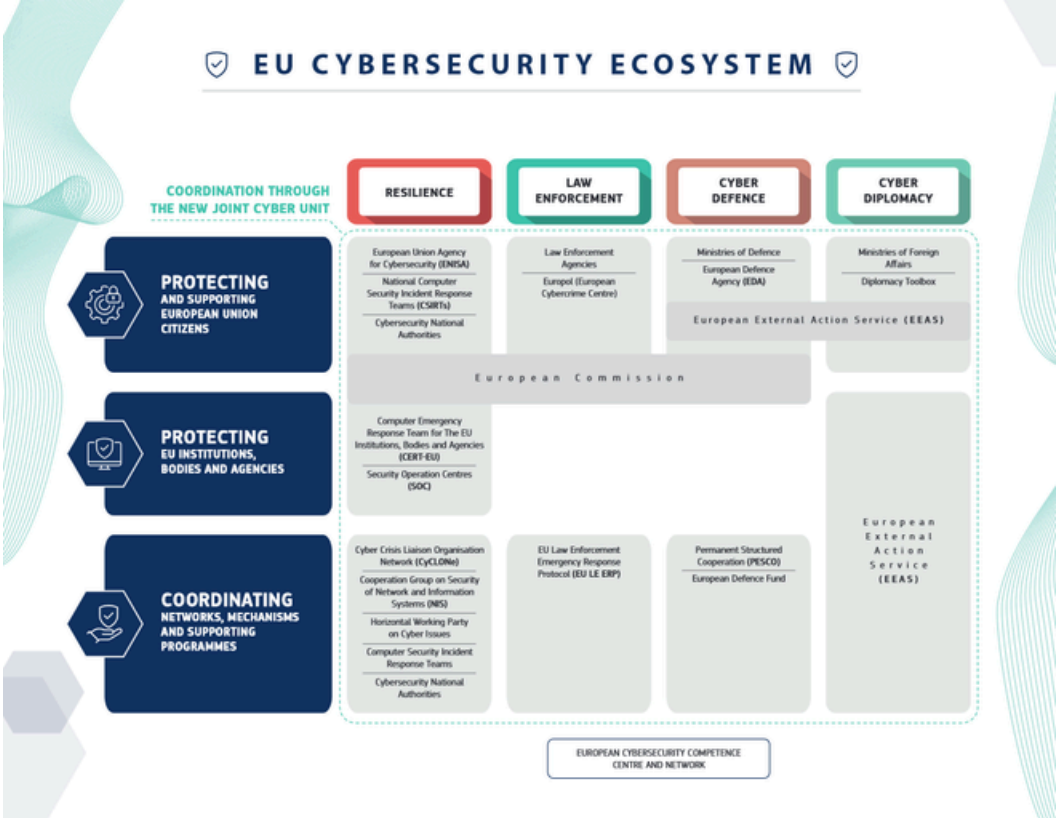
A análise que se vai fazer adiante centra-se na Diretiva "SRI 2". Este ato introduz modificações significativas no regime previsto na Diretiva "SRI 1", seja mediante o alargamento do âmbito subjetivo dos setores abrangidos, seja no que respeita ao regime de supervisão e controlo e ao regime sancionatório. Os objetivos podem resumir-se a uma tríade de missões: i) o aumento do nível de resistências cibernética de um conjunto mais abrangente de empresas que operam na União, em todos os setores relevantes, visando a capacidade de resposta de entidades públicas e privadas e da sociedade no seu conjunto; ii) a redução das incoerências detetadas nos setores já abrangidos; e iii) a sensibilização ou o aumento do nível de consciência conjunto e de capacidade coletiva de preparação e resposta, nomeadamente através da articulação e do aumento da confiança entre autoridades competentes, fomentando a sua capacidade de resposta a crises de grande escala.A Comissão afirma que a Diretiva "SRI 1" não foi capaz de impedir diferenças substanciais entre os EM no que respeita à resiliência dos vários setores, demonstrando particular preocupação com as PMEs, com as infraestruturas de cabos e desenvolvimentos recentes como as cidades inteligentes.

No que tange ao quadro institucional, desta feita começando pela UE, a estrutura de governação tem-se alargado em diferentes vertentes e com diferentes missões:

- Resiliência: O organismo responsável pela cibersegurança das instituições, agências e órgãos da UE, CERT-EU (The Computer Emergency Response Team for the EU institutions, bodies and agencies); CSIRTs Network, estabelecida pela Diretiva "SRI 1" e reforçada pela "SRI 2", é uma rede composta pelas CSIRT (Computer Security Incident Response Team) nacionais e pela CERT-EU; a rede EU-CyCLONe (European cyber crisis liaison organisation network), lançada em 2020 e agora prevista no artigo 16.º da Diretiva "SRI 2", com o objetivo principal de assegurar uma resposta eficiente a incidentes com impacto transnacional; o Grupo de Cooperação em Redes e Sistemas de Informação foi criado pela Diretiva SRI para assegurar a cooperação e o intercâmbio de informações entre os Estados-Membros; o EU-ISAC, para apoiar os Information Sharing and Analysis Centres nos diversos setores económicos; o European Cyber shield composto pelos Security Operations Centres (SOCs) avançado, em abril de 2023, na proposta de Regulamento "Ciber solidariedade" [COM(2023) 209 final]; o Grupo de Certificação de cibersegurança da UE (ECCG);
- Efetivação jurídica: o European Cyber Crime Centre da EUROPOL (EC3) para o combate ao cibercrime, articulado com o quadro operacional da Joint Cyber Crime Taskforce (JCAT), que envolve autoridades de 13 EM e de sete Estados parceiros;
- Diplomacia: o Serviço Europeu de Ação Externa (SEAE); o Horizontal Working Party on Cyber Issues, que é responsável pela coordenação da política e legislação do Conselho em matéria de cibersegurança; o Centro de Inteligência e de Informação da UE (EU INTCEN); o EU Cyber Diplomacy Toolbox;
- Defesa: a Single Intelligence Analysis Capacity (SIAC) combina a inteligência civil (EU INTCEN) e a inteligência militar (EUMS Intelligence Directorate);
- Educação: o Centro Europeu de Competências em Cibersegurança, em Bucareste e a Cybersecurity Skills Academy.

Acresce a importância das estruturas de associação e representação da indústria, em que se salienta a ECSO[38] (Organização Europeia para a Cibersegurança / European Cyber Security Organisation), entidade de tipo associativo que federa privados e públicos, nacionais e europeus.

Esta multiplicidade de estruturas deverá ser articulada através da plataforma Ciberunidade conjunta («*Joint Cyber Unit*») que reúne a ENISA, o *European Cybercrime* Centre («EC3») da Europol, a Equipa de Resposta a Emergências Informáticas para as instituições, organismos e agências da UE («CERT UE»), a Comissão, o Serviço Europeu para a Ação Externa (incluindo o INTCEN), a rede de CSIRT e a UE CyCLONe, a Agência Europeia de Defesa , o presidente do Grupo de Cooperação SRI, o presidente do Grupo Horizontal do Conselho das Questões do Ciberespaço e um representante dos projetos relevantes da PESCO. Foi previsto o envolvimento dos *stakeholders* privados a partir de junho de 2023.



Fonte: European Commission
https://digital-strategy.ec.europa.eu/en/library/infographic-eu-cybersecurity-ecosystem
[último acesso em 23.02.2024]

Este quadro institucional europeu integra e articula-se com um quadro institucional paralelo dos EM.

Em Portugal, a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 estabelece o quadro fundamental sobre o qual atuam e se articulam o Conselho Superior de Segurança do Ciberespaço, o Centro Nacional de Cibersegurança (CNCS), enquanto autoridade nacional de cibersegurança , e outras entidades com competências transversais ou setoriais, como o Ministério Público, a Polícia Judiciária, as Forças Armadas, o Sistema de

[38] https://ecs.org.eu [último acesso em 26.03.2024].

Informações da República Portuguesa e o Sistema de Segurança Interna, bem como a equipa de resposta a incidentes de segurança informática nacional «CERT.PT», serviço integrante do CNCS, que é também membro da Rede Nacional de CSIRT e representante nacional da Rede Europeia de CSIRT estabelecida pela Diretiva (UE) 2016/1148. O Despacho n.º 11491/2022, de 28 de setembro, designa o Centro Nacional de Cibersegurança como centro nacional de coordenação para efeitos do Regulamento (UE) 2021/887 e cria o consórcio entre o CNCS, a Agência Nacional de Inovação e a Fundação da Ciência e Tecnologia. Portugal conta com cinco Centros de Análise e Partilha de Informação (ISAC), dinamizados pelo CNCS, para a recolha, análise e partilha de informação entre operadores e instituições "primordiais ao regular funcionamento económico e político"[39], que têm atuado nos setores da energia, das águas, portos marítimos, media e retalho e distribuição; estão em preparação outros ISACs em outros setores de atividade e para as regiões autónomas. Já a rede nacional de CSIRTs reúne equipas de resposta a incidentes da administração pública, da academia, do setor financeiro, da energia, comunicações e indústria, e desenvolve indicadores e recomendações para promover uma cultura de cibersegurança e a capacidade de resposta a incidentes de larga escala.

Tal como o quadro legislativo e regulatório, este ecossistema institucional nacional e as respetivas competências e funcionamento são presentemente objeto de modificação, em conformidade com o novo regime regulatório da União. Nos EM, nomeadamente em Portugal, será oportuno fazer acompanhar a implementação da Diretiva "SRI 2" da elaboração da nova Estratégia Nacional de Segurança do Ciberespaço para depois de 2023.

3. A REGULAÇÃO EUROPEIA DA CIBERSEGURANÇA – A NOVA DIRETIVA "SRI 2"

A Diretiva (UE) 2016/1148 (também conhecida por Diretiva "SRI 1") foi o primeiro ato legislativo europeu para a cibersegurança. Este ato tinha por objetivo o desenvolvimento de capacidades de cibersegurança na União Europeia, a atenuação de ameaças aos sistemas de rede e informação em serviços de setores-chave e a garantia da continuidade dos serviços em face de incidentes[40].

A despeito dos progressos alcançados, a Diretiva (UE) 2016/1148 revelou-se incapaz de responder eficazmente aos desafios atuais e emergentes no domínio da cibersegurança em um contexto de rápida transformação digital e de intercâmbios transfronteiriços[41]. A Comissão Europeia[42] refere que a transformação digital da sociedade, intensificada pela pandemia, exige novas respostas. A avaliação da sua aplicação revelou a insuficiência do seu âmbito de aplicação, a incerteza sobre as entidades abrangidas, a disparidade dos requisitos de segurança e dos regimes de notificação de incidentes entre os EM, bem como uma supervisão e sancionamento lenientes. Também a colaboração entre as autoridades e com os operadores privados não se tinha concretizado como desejável. Finalmente, a realidade demonstrava um nível de maturidade na gestão de riscos de

[39] Para mais informação, veja-se https://www.cncs.gov.pt/pt/isac/ [último acesso em 23.02.2024].
[40] Considerando n.º 1 da Diretiva (UE) 2022/2555.
[41] Considerandos n.º 2 e n.º 3 da Diretiva (UE) 2022/2555.
[42] COM(2020) 823 final, p. 1.

cibersegurança e de ciber-resiliência muito variáveis entre os EM[43].

A Diretiva (UE) 2022/2555 surge para responder a esses desafios e impõe uma modificação do regime jurídico da cibersegurança vigente nos Estados Membros da União Europeia, a concluir até 17 de outubro de 2024. Há que mencionar que a Diretiva (UE) 2022/2555 não é um ato normativo isolado; pelo contrário, foi elaborada num contexto de reforço da resposta aos riscos para a segurança na União Europeia, em sentido *lato*, tendo sido publicada em 14 de dezembro de 2022, juntamente com a Diretiva (UE) 2022/2557, a Diretiva (UE) 2022/2556 e o Regulamento (UE) 2022/2554 (que compõem o designado «Cybersecurity Package».

A Diretiva (UE) 2022/2557 refere-se à resiliência das entidades críticas e ocupa-se de riscos naturais e de origem humana, incluindo aqueles de natureza intersetorial ou transfronteiriça, que possam afetar a prestação de serviços essenciais, tais como acidentes, catástrofes naturais, emergências de saúde pública, ameaças híbridas ou outras ameaças antagónicas, incluindo terrorismo, infiltrações criminosas e sabotagens. Por sua vez, a Diretiva (UE) 2022/2556 e o Regulamento (UE) 2022/2554 tratam da resiliência operacional digital para o setor financeiro.

Nesse contexto, a Diretiva (UE) 2022/2557 preocupa-se com riscos gerais à segurança da União, enquanto, de um lado, a Diretiva (UE) 2022/2555 e, de outro, a Diretiva (UE) 2022/2556 e o Regulamento (UE) 2022/2554 preocupam-se com riscos específicos, quais sejam, respectivamente, a cibersegurança e a segurança do setor financeiro. A conexão demanda uma atuação coordenada das autoridades competentes, ao nível nacional ou supranacional[44].

Os propósitos da Diretiva 2022/2555, em vigor desde janeiro de 2023, são abrangentes, mas podem resumir-se como uma abordagem integrada dos principais setores com impacto económico e social fundamental, seja para os indivíduos, seja para a sociedade. Altera o Regulamento (EU) n.º 910/2014 e a Diretiva (EU) 2018/1972, mas, sobretudo, revoga a Diretiva (EU) 2016/1148 (Diretiva "SRI 1"). O seu título logo indicia uma maior clareza e precisão do seu objeto – a adoção de "medidas destinadas a garantir um elevado nível comum de cibersegurança", em vez de "medidas destinadas a garantir um elevado nível comum de segurança de redes de informação". Alarga o âmbito de aplicação da Diretiva revogada (de trinta, passam a estar abrangidas sessenta e sete tipos de entidades) e promove a consolidação de um quadro nacional e supranacional de autoridades competentes nesse domínio e respetiva colaboração, incrementando o nível de harmonização em relação aos requisitos de segurança e às obrigações dos Estados Membros.

Ainda que continue a ser uma Diretiva de harmonização mínima, como a anterior, em linhas gerais, a Diretiva "SRI 2" reduz a margem de apreciação dos Estados-Membros e traz inovações nos seguintes aspetos:

a) um âmbito significativamente alargado e padronizado, com o fim de obter maior uniformidade e coerência nas legislações dos Estados-Membros;

[43] No National Cyber Security Index, índice da capacidade dos países para prevenir e gerir incidentes de cibersegurança, com base em políticas públicas, Portugal, a nível mundial, evoluiu do 16.º lugar em 2019 (com 64% de pontuação) para 8º em 2023 (com 90%). https://ncsi.ega.ee/ncsi-index/?order=rank&type=c&archive=1 [último acesso em 23.02.2024].
[44] Dentre tantas manifestações nesse sentido presentes na Diretiva (UE) 2022/2555, menciona-se, como exemplos, os artigos 2.º, n.º 12, 14.º e 37.º.

b) uma nova classificação das entidades, segundo o critério de essencialidade e de importância, todas elas consideradas críticas;

c) a criação de regimes diferenciados de supervisão e execução, de acordo com a classificação da entidade, introduzindo a modalidade de supervisão *ex ante* para as entidades essenciais, com o intento preventivo de incidentes, além de novas obrigações;

d) a exigência de designação ou criação de autoridades para integrar um quadro nacional de gestão de cibercrises e aumento das funções atribuídas ao grupo de cooperação a nível da União, incluindo um ponto de contacto único;

e) a intensificação das medidas de gestão e cooperação quanto aos riscos e incidentes de cibersegurança, atuais ou potenciais.

O cotejo das regras correspondentes entre a "SRI 1" e a "SRI 2", com respaldo na tabela que consubstancia o Anexo III da Diretiva (UE) 2022/2555, evidencia o nível de pormenorização almejado neste novo ato normativo, seja em razão do grau de minúcia adotado em comparação à Diretiva revogada, seja em razão da inserção de várias regras não previstas anteriormente. É evidente que o regime se tornou mais exigente e exaustivo.

No nível europeu, a diretiva reforçou o quadro de governação, seja aumentando as atribuições da ENISA, seja promovendo a coordenação estratégica através do grupo de cooperação do EU-CyCLONe.

3.1. ÂMBITO SUBJETIVO DE APLICAÇÃO

A nova Diretiva procedeu a um alargamento significativo das entidades abrangidas, a par com a modificação da sua classificação. São vários os novos setores e subsetores submetidos ao regime instituído pela Diretiva. A indispensável adaptação importará custos elevados, tal como é expectável que se intensifique o recurso a seguros de responsabilidade civil.

O primeiro recorte das entidades abrangidas é definido pela natureza crítica do respetivo setor de atividade e resulta da articulação entre o artigo 2.º e os Anexos I e II. Os Anexos indicam os setores (e subsetores) de importância crítica (Anexo 1: Energia; Transportes; Setor Bancário; Infraestruturas do mercado financeiro; Saúde; Água potável; Águas residuais; Infraestruturas digitais; Gestão de serviços TIC (entre empresas); Administração pública; e, Espaço) e outros setores críticos (Anexo 2: Serviços postais e de estafeta; Gestão de resíduos; Produção, fabrico e distribuição de produtos químicos; Produção, transformação e distribuição de produtos alimentares; Indústria transformadora[45]; Prestadores de serviços digitais; Investigação). Ao proceder a uma comparação genérica, percebe-se que os setores incluídos no atual Anexo I (Setores de Importância Crítica) correspondem aos setores incluídos no Anexo II da Diretiva "SRI 1" (Operadores de serviços essenciais), mas incluem mais subsetores (v.g., na Energia, o

[45] Sobre as atividades incluídas na indústria transformadora, veja-se https://smi.ine.pt/Categoria/Detalhes/2859887?modal=1 [último acesso em 26.03.2024]. Segundo o CAE, "[a]s indústrias transformadoras caracterizam-se, em termos genéricos, como actividades que transformam, por qualquer processo (químico, mecânico, etc.), matérias-primas provenientes de várias actividades económicas (inclui materiais usados e desperdícios) em novos produtos. A alteração, renovação ou reconstrução substancial de qualquer bem, considera-se parte integrante das indústrias transformadoras." Disponível em https://eportugal.gov.pt/categorias-de-actividade/transformadoras [último acesso em 26.03.2024].

hidrogénio) e novos setores (Águas residuais; Gestão de Serviços TIC; Administração Pública central e regional; Espaço). Já o Anexo II inclui os serviços digitais anteriormente previstos no Anexo III da Diretiva "SRI 1", mas acrescenta um número significativo de novos setores, não abrangidos no âmbito subjetivo do ato agora revogado.

O elemento determinante seguinte é a dimensão ou o impacto socioeconómico. Segundo o artigo 2.º, n.º 1, a diretiva aplica-se às entidades dos setores elencados nos Anexos I e II, sejam públicas ou privadas, que sejam médias empresas ou estejam acima do respetivo limiar, nos termos do artigo 2.º do anexo da Recomendação 2003/361/CE.

Independentemente da respetiva dimensão, a diretiva abrange as entidades dos tipos mencionados nas seguintes situações (n.º 2 do artigo 2.º):

a) Os serviços são prestados por: i) fornecedores de redes públicas de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público, ii) prestadores de serviços de confiança, iii) registos de nomes de domínio de nível superior (TLD) e prestadores de serviços de sistemas de nomes de domínio (DNS);

b) A entidade é o único prestador, num Estado-Membro, de um serviço que é essencial para a manutenção de atividades societais ou económicas críticas;

c) Uma perturbação do serviço prestado pela entidade possa afetar consideravelmente a segurança pública, a proteção pública ou a saúde pública;

d) Uma perturbação do serviço prestado pela entidade possa gerar riscos sistémicos consideráveis, especialmente para os setores onde tal perturbação possa ter um impacto transfronteiriço;

e) A entidade é crítica devido à sua importância específica, a nível nacional ou regional, para o setor ou o tipo de serviço em causa, ou para outros setores interdependentes no Estado-Membro;

f) A entidade é uma entidade da administração pública: i) do governo central, tal como definida por um Estado-Membro em conformidade com o direito nacional, ou ii) a nível regional, tal como definida por um Estado-Membro em conformidade com o direito nacional, que, na sequência de uma avaliação baseada no risco, presta serviços cuja perturbação seria suscetível de ter um impacto significativo nas atividades societais ou económicas críticas.

Estipula o artigo 2.º, n.º 3 que também as entidades identificadas como entidades críticas segundo a Diretiva (UE) 2022/2557 estão abrangidas pela Diretiva 2022/2555, independentemente da respetiva dimensão. Os setores elencados neste último ato coincidem em grande medida, embora com designações não necessariamente idênticas, com as categorias incluídas no Anexo I e uma categoria incluída no Anexo II da Diretiva "SRI 2", o que retira relevância ao critério da dimensão, alargando a abrangência da Diretiva "SRI 2". Assim, comparando os respetivos âmbitos, das categorias previstas no Anexo I da Diretiva "SRI 2" apenas estão excluídas das categorias da Diretiva 2022/2557 as entidades de "Gestão de Serviços TIC". Por outro lado, entre as entidades acrescentadas naquela cláusula e que, portanto, ficam abrangidas independentemente da respetiva dimensão, encontram-se as seguintes: i) no subsetor dos transportes

rodoviários, entidades que operam transportes públicos na aceção do artigo 2.º, alínea d), do Regulamento (CE) n.o 1370/2007 do Parlamento Europeu e do Conselho; ii) no setor da saúde, as entidades titulares de uma autorização de distribuição a que se refere o artigo 79.º da Diretiva 2001/83/CE. Para além destas, é considerada uma categoria de entidades críticas pela Diretiva 2022/2557 o setor da "Produção, transformação e distribuição de produtos alimentares", categoria que na Diretiva "SRI 2" integra o Anexo II.

O n.º 4 prevê idêntica regra de sujeição independentemente da dimensão para as entidades prestadoras de serviços de registo de nomes de domínio.

Já as entidades da Administração Pública local e as instituições de ensino podem ser submetidas pelos EM ao regime da Diretiva (n.º 5).

Em sentido inverso, os n.os 6 a 8 afastam do âmbito da Diretiva, imediata ou mediatamente, total ou parcialmente, entidades relacionadas com a defesa, segurança nacional ou segurança pública, incluindo a investigação e ação penal. Neste regime excecional, não se abrangem entidades que atuem como prestadores de serviços de confiança.

Também se aplica a Diretiva "SRI 2" às entidades previstas no artigo 2.º, n.º 5, pontos 4) a 22) da Diretiva 2013/36/UE que os EM tenham excluído da aplicação do Regulamento «DORA» (Regulamento (UE) 2022/2554), *ex vi* do artigo 2.º n.º 10.

3.2. UM REGIME DE HARMONIZAÇÃO MÍNIMA, SUBSIDIÁRIO E DIFERENCIADO

Tal como a anterior, a Diretiva "SRI 2" é uma diretiva de harmonização mínima (artigo 5.º), que admite que os EM imponham um regime de garantia da cibersegurança mais elevado, seja impondo exigências mais elevadas, seja alargando o âmbito de entidades abrangidas. Este, no entanto, deve respeitar as obrigações resultantes do DUE, em especial os princípios da não discriminação e as liberdades do mercado interno.

Além disso, a Diretiva "SRI 2" institui um regime transversal subsidiário que ressalva medidas tão ou mais exigentes impostas pela União em atos de natureza setorial (artigo 4.º, n.ºs 1 e 2). O n.º 3, por sua vez, determinou que a Comissão, com o apoio da ENISA, publicaria, até 17 de julho de 2023, orientações para a clarificação dos números anteriores. Estas foram apresentadas na Comunicação 2023/C 328/02, publicada no JO C 328/2, no dia 18.9.2023, onde, além da densificação de definições e conceitos como «segurança dos sistemas de rede e informação» ou «ameaça», se indica como ato setorial relevante cujo regime especial prevalece o Regulamento (UE) 2022/2554 (Regulamento «DORA»).

Não obstante ser transversal e incluir no seu âmbito de aplicação os "setores de importância crítica", elencados no Anexo I, e "outros setores críticos" , elencados no Anexo II, o regime aplicável às entidades abrangidas é diferenciado.

O conjunto de entidades abrangidas é segmentado em em dois grupos distintos de entidades abrangidas, que o artigo 3.º da Diretiva "SRI 2" denomina, respetivamente, de

"essenciais" (n.º 1) e "importantes" (n.º 2). Esta classificação reflete-se em regimes distintos para cada categoria, contemplando-se, medidas de supervisão e de execução reforçadas ou sanções mais graves para as entidades essenciais, tal como se verá adiante.

Em vez da categoria de «operadores de serviços essenciais» e e «prestadores de serviços digitais», categorias relevantes na Diretiva "SRI 1" - artigo 1,º, n.º 2, al. d) -, o novo regime reflete a integração do digital em todos os setores de atividade e assenta a nova distinção em critérios de relevância socioeconómica, de dimensão e do impacto significativo das respetivas atividades na economia e sociedade. Na verdade, há uma continuidade, pois os operadores dos serviços essenciais na Diretiva "SRI 1" eram as entidades abrangidas no Anexo II e, como tal, correspondem tendencialmente às entidades agora qualificadas como entidades essenciais.

As entidades essenciais são, em primeiro lugar, as entidades de um dos tipos do Anexo I (desde que cumpram o requisito do limiar de média empresa, de acordo com o artigo 3.º, n.º 1, al. a). Igualmente, sujeitos ao mesmo requisito de dimensão, são entidades essenciais os fornecedores de redes públicas de comunicações eletrónicas, prestadores de serviços de comunicações eletrónicas acessíveis ao público (artigo 3,º, n.º 1, al. c)). Independentemente da respetiva dimensão, são qualificadas como entidades essenciais, as entidades identificadas como entidades críticas pela Diretiva 2022/2557 (artigo 3.º, n.º 1, al. f)), os prestadores de serviços de confiança qualificados e registos de nomes TLD, os prestadores de serviços de DNS (artigo 3.º, n.º 1 al.b)), as entidades da administração pública central (artigo 3.º, n.º 1, al. d)). A estas somam-se as entidades pertencentes aos setores indicados nos dois anexos, e que sejam assinaladas pelos EM como essenciais, nos termos do artigo 2.º, n.º 2, alíneas. b) a e) ex vi do artigo 3.º, n.º 1, al. e), por serem o único prestador num EM de um serviço que é essencial para a manutenção de atividades societais ou económicas críticas, pelo facto de uma perturbação do serviço que prestam poder afetar consideravelmente a segurança pública, a proteção pública ou a saúde pública, poder gerar riscos sistémicos consideráveis, em especial transfronteiriços, ou, ainda, devido à sua importância específica, a nível nacional ou regional, para o setor ou tipo de serviço em causa ou para outros setores interdependentes. Integram ainda a categoria de entidades essenciais, as entidades identificadas pelos EM como operadores de serviços essenciais antes de 16 de janeiro de 2023.

A categoria das entidades importantes pode resultar, para as entidades previstas no artigo 2.º, n.º 2, alíneas b) a e), da classificação como tal pelos EM, e abrange ainda todas as outras que são referidas nos anexos I e II e que não sejam essenciais (artigo 3.º, n.º 2).

O artigo 3.º, n.º 3 impõe aos EM a elaboração de uma lista das entidades essenciais e importantes e das entidades que prestam serviços de registo de nomes de domínio, lista onde devem constar as informações constantes do n.º 4. Essa lista deve ser atualizada com regularidade e, pelo menos, bienalmente. O n.º 5 impõe deveres de comunicação à Comissão.

Um dos objetivos da presente diretiva foi reduzir a margem de apreciação antes conferida pela Diretiva (UE) 2016/1148 aos Estados-Membros, dada a conclusão de que estes implementaram a diretiva anterior de modo significativamente diferente, a exemplo do que ocorreu nos campos das obrigações de notificação e medidas de supervisão e execução[46]; isto não significa, contudo, que a margem de apreciação dos Estados-

[46] Considerando n.º 4 da Diretiva (UE) 2022/2557.

Membros foi excluída. Na verdade, considerando o referido artigo 5.º e a natureza de cláusulas gerais e o caráter indeterminado de vários dos conceitos utilizados nas disposições mencionadas, os EM continuarão a ter uma significativa latitude, ainda que as orientações da Comissão, nos termos do artigo 3.º, n.º 4[47], e o registo na referida lista contribuam para a certeza e para reduzir a discricionariedade estadual.

Por último, para o recorte das entidades abrangidas não é determinante a sua sede europeia. Efetivamente, a aplicação do novo regime é reforçada através do regime imposto às entidades não situadas no território da UE. Estas, quando prestem serviços na UE, não só ficam submetidas ao regime da União como devem nomear um representante num dos EM, ficando submetidas à fiscalização das autoridades desse Estado (artigo 26.º).

4. EIXOS DO REGIME JURÍDICO DE CIBERSEGURANÇA INSTITUÍDO PELA DIRETIVA (UE) 2022/2555

O regime jurídico imposto pela Diretiva (UE) 2022/2555 às entidades por ela abrangidas desenvolve-se em quatro eixos principais. São eles: i) medidas de gestão de riscos de cibersegurança (artigos 21º e 24º); ii) obrigações de notificação e comunicação (artigo 23º); iii) medidas de supervisão e execução (artigos 31º a 33º); e iv) sanções (artigo 34º a 36º).

Sucintamente, o escopo do regime instituído é em primeiro lugar a prevenção de incidentes e de seguida, verificado um incidente, a máxima minimização e mitigação dos respetivos danos. Impõem-se ações nacionais de preparação, incluindo exercícios e atividades de formação e de um plano nacional de resposta a crises e a incidentes de cibersegurança (artigo 9.º).

4.1. MEDIDAS DE GESTÃO DE RISCO DE CIBERSEGURANÇA

As medidas de gestão de riscos de cibersegurança consistem em medidas técnicas, operacionais e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança dos sistemas de rede e informação que as entidades essenciais e importantes utilizam nas suas operações ou na prestação dos seus serviços e para impedir ou minimizar o impvacto de incidentes nos destinatários dos seus serviços e noutros serviços, como dispõe dispõe o artigo 21º, nº 1, da Diretiva (UE) 2022/2555. Essas medidas incluem a identificação de ativos críticos, avaliação de vulnerabilidades e ameaças, implementação de políticas de análise de risco e de segurança dos sistemas de informação e adoção de mecanismos de comunicação direta e de notificação de informações obrigatórias às autoridades competentes.

A Diretiva “SRI 2” reforçou esta dimensão fundamental da cibersegurança, com o objetivo primeiro de melhorar a prevenção e assegurar a resiliência contra ameaças e ataques. Estas medidas devem ser incluídas pelas entidades abrangidas pela diretiva no quadro de

[47] Estas orientações foram apresentadas na Comunicação da Comissão 2023/C 324/02, publicada no JO C 324/2, de 14.9.2023.

governação, conforme previsto no artigo 20.º da Diretiva, segundo o qual os órgãos de direção das entidades essenciais e importantes aprovam as medidas de gestão dos riscos de cibersegurança tomadas por essas entidades, supervisionam a sua aplicação e podem mesmo ser responsabilizados por eventuais infrações praticadas pelas entidades (artigo 20.º, n.º 1). Trata-se de um verdadeiro programa de governação corporativa e *compliance* em cibersegurança, que inclui não apenas práticas de ciber-higiene, mas também medidas proativas de formação e relativas à gestão de incidentes, à continuidade das atividades, à segurança da cadeia de abastecimento, e à segurança na aquisição, desenvolvimento e manutenção de redes e sistemas de informação. Deve conter, no mínimo, o comprometimento dos órgãos de gestão das entidades, a aprovação das medidas técnicas, operacionais e organizativas pertinentes, a supervisão da sua aplicação, a responsabilização, no âmbito da entidade, por infrações cometidas (artigo 20.º, n.º 1), a participação obrigatória dos membros dos órgãos de direção em ações de formação em cibersegurança e o incentivo a que todos os trabalhadores da entidade também participem de ações de formação desta natureza (artigo 20.º, n.º 2). Os órgãos de gestão das entidades abrangidas podem ser responsabilizados pelo não cumprimento destas obrigações.

O artigo 21.º, n.º 2, da diretiva dispõe que as medidas de gestão devem abranger, pelo menos, os seguintes aspetos: a) políticas de análise dos riscos e de segurança dos sistemas de informação; b) tratamento de incidentes; c) continuidade das atividades, como a gestão de cópias de segurança e a recuperação de desastres, e gestão de crises; d) segurança da cadeia de abastecimento, incluindo aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços diretos; e) segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação, incluindo o tratamento e a divulgação de vulnerabilidades; f) políticas e procedimentos para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança; g) práticas básicas de ciber-higiene e formação em cibersegurança; h) políticas e procedimentos relativos à utilização de criptografia e, se for caso disso, de cifragem; i) segurança dos recursos humanos, políticas seguidas em matéria de controlo do acesso e gestão de ativos; j) utilização de soluções de autenticação multifatores ou de autenticação contínua, comunicações seguras de voz, vídeo e texto e sistemas seguros de comunicações de emergência no seio da entidade, se for caso disso.

Tudo isto sem prejuízo da possibilidade de os Estados-membros, estabelecerem medidas de gestão adicionais, não previstas na diretiva, para as entidades abrangidas.

Deve salientar-se que a diretiva não estabelece qualquer distinção entre as medidas de gestão a serem adotadas pelas entidades essenciais e pelas entidades importantes. Isto não quer dizer, contudo, que não deva haver diferenciação e a imposição de um regime mais exigente a algumas entidades. Os EM podem e devem fazê-lo na concretização das medidas técnicas, operacionais e organizativas que lhe competem, utilizando uma abordagem material, setorial e casuística. O artigo 21.º, n.º 1 aponta aos Estados como critério a adequação e proporcionalidade em função dos "riscos que se colocam à segurança dos sistemas de rede e informação que utilizam nas suas operações ou na prestação dos seus serviços e para minimizar o impacto de incidentes nos destinatários dos seus serviços e noutros serviços" (§ 1) e para tal "deve ser tido em devida conta o grau de exposição da entidade aos riscos, a dimensão da entidade e a probabilidade de ocorrência de incidentes e a sua gravidade, incluindo o seu impacto social e económico" (§ 2). Quanto aos requisitos técnicos e metodológicos das medidas previstas no artigo

21.º, n.º 2, a sua definição para os prestadores de serviços de DNS, os registos de nomes de TLD, os prestadores de serviços de computação em nuvem, os prestadores de serviços de centro de dados, os fornecedores de redes de distribuição de conteúdos, os prestadores de serviços geridos, os prestadores de serviços de segurança geridos, bem como os prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais e os prestadores de serviços de confiança, serão adotados pela Comissão até 17/10/2024 (artigo 21.º, n.º 5 § 1); a Comissão tem ainda a faculdade de determinar tais requisitos para as outras entidades essenciais e importantes (artigo 21.º, n.º 5, § 2).

Por outro lado, no seu artigo 24.º, n.º 1, a diretiva permite que os EM obriguem as entidades essenciais e importantes a utilizar determinados produtos de TIC, serviços de TIC e processos de TIC, desenvolvidos pela própria entidade essencial ou importante ou fornecidos por terceiros, que estejam certificados no âmbito de sistemas europeus de certificação da cibersegurança adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881. O n.º 2 habilita a Comissão a adotar atos delegados que especifiquem as categorias de entidades obrigadas a utilizar produtos de TIC, serviços de TIC e processos de TIC certificados ou a obter um certificado ao abrigo de um sistema europeu de cibersegurança. A elaboração desses atos delegados deve ser realizada em colaboração com o grupo de cooperação e com a ENISA (artigo 21.º, n.º 5, § 3). É salutar a elaboração desses atos de execução, pois fornecem balizas técnicas, metodológicas e setoriais para a elaboração das medidas de gestão de riscos em cibersegurança, de modo a contribuir para o cumprimento da diretiva de modo mais uniforme e, consequentemente, mais eficaz para o efetivo incremento do nível de cibersegurança na União Europeia.

No contexto da governação multinível, este é um evidente exemplo de articulação da regulação vinculante com os organismos de estandardização. Esta é uma questão bastante relevante, a respeito da qual o Estado português deverá decidir: para efeito de cumprimento do estabelecimento de medidas de gestão de riscos de cibersegurança, que entidades abrangidas pela diretiva deverão estar obrigadas a utilizar determinados produtos de TIC, serviços de TIC e processos de TIC certificados no âmbito de sistemas europeus de certificação da cibersegurança? Parece-nos que a escolha pela exigência de certificação é benéfica e contribui para a elevação do nível de segurança cibernética na União, embora possa acarretar custos superiores.

4.2. OBRIGAÇÕES DE NOTIFICAÇÃO E COMUNICAÇÃO

A diretiva “SRI 2” não estabelece regimes jurídicos diferentes entre entidades essenciais e importantes para as obrigações de notificação e comunicação. O artigo 23.º, n.º 1 da Diretiva “SRI 2” impõe às entidades a obrigação de notificarem qualquer incidente significativo, i.e. um incidente que tenha um impacto significativo na prestação dos, seus serviços à equipa de resposta a incidentes de segurança informática (CSIRT) ou, se aplicável, à autoridade competente. Esta obrigação de “reporting” é reforçada em relação ao regime anterior.

O conceito de “incidente significativo” é um conceito indeterminado que necessita de preenchimento. Não se trata de um conceito de natureza quantitativa ou sequer material. O n.º 3 do artigo 23.º considera um incidente significativo se: a) tiver causado ou for suscetível de causar graves perturbações operacionais dos serviços ou perdas financeiras à entidade em causa; b) tiver afetado ou for suscetível de afetar outras pessoas singulares

ou coletivas, causando danos materiais ou imateriais consideráveis. Esta densificação feita pela diretiva é a possível, ainda que seja insuficiente, porquanto composta por cláusulas gerais integradas por conceitos também indeterminados, como "danos consideráveis" e "graves perturbações". Por esta razão, a Comissão tem, por um lado, o dever de adotar atos de execução, até 17/10/2024, que especifiquem os casos em que um incidente deve ser considerado significativo, para tipos específicos de entidades dos setores de infraestruturas digitais, bem como para as entidades dos setores de gestão de serviços TIC entre empresas e prestadores de serviços digitais (artigo 23.º, n.º 11, § 2 combinado com os itens 8 e 9 do Anexo I e item 6 do Anexo II); por outro lado, tem a faculdade de adotar atos de execução de mesma natureza em relação a outras entidades essenciais e importantes (artigo 23.º, n.º 11, § 2).

O procedimento de notificação de incidente significativo ocorre por meio da emissão de um alerta, do envio de uma notificação e da apresentação de relatórios. Em primeiro lugar, impõe-se, a emissão de um alerta rápido, 24 horas após o conhecimento do incidente (artigo 23.º, n.º 4, al. a); depois disso, deve ser efetuada a notificação de incidente, 72 horas após o conhecimento do incidente (artigo 23.º, n.º 4, al. b); e, depois, exige-se a apresentação de um relatório final, o mais tardar um mês após a notificação de incidente ou após a resolução do incidente, com o respetivo conteúdo mínimo a ser definido na diretiva (artigo 23.º, n.º 4, al. d). Eventualmente, exige-se a elaboração de relatório intercalar, quando a CSIRT ou autoridade competente entender que se verifica a necessidade de prestação de informações atualizadas ou quando ao tempo da elaboração do relatório final o incidente ainda esteja em curso, caso em que em lugar do relatório final se apresenta o relatório intercalar e, até um mês após a resolução do incidente, apresenta-se o relatório final (artigo 23.º, n.º 4, als. c) e e)).

Merece atenção, como derivação do valor da transparência[48], a obrigação para as entidades essenciais e importantes de informar os destinatários dos seus serviços. Assim, devem i) comunicar sem demora, os incidentes significativos suscetíveis de afetar negativamente a prestação desses serviços (artigo 23.º, n.º 1, § 1); ii) quando aplicável, prestar informação acerca da própria ciberameaça significativa e das medidas ou soluções que os destinatários podem adotar para responder a essa ameaça (artigo 23.º, n.º 2). A Comissão tem a faculdade de adotar atos de execução de mesma natureza em relação a outras entidades essenciais e importantes (artigo 23.º, n.º 11, § 2). Esses atos de execução devem ser elaborados com a colaboração do grupo de cooperação (artigo 23.º, n.º 11, § 3), observado o procedimento instituído pelo artigo 5.º do Regulamento n.º 182/2011 da União Europeia (artigo 23.º, n.º 11, § 4).

A adoção dos referidos atos de execução vai permitir uma aplicação mais uniforme do regime previsto na diretiva, seja pelas autoridades estaduais, seja pelas entidades abrangidas, e vai contribuir para a certeza jurídica, favorecendo a cibersegurança no espaço europeu.

4.3. SUPERVISÃO E EXECUÇÃO

Estas competências são atribuídas às autoridades competentes dos EM, que têm de assegurar o cumprimento da diretiva. O novo regime é bastante pormenorizado. Ao

[48] Este valor, essencial em domínios em que o risco de um sistema pode afetar significativamente terceiros, como clientes e fornecedores, e as dificuldades e a ponderação de interesses e benefícios que implica, exigem uma avaliação ética casuística complexa e fundamentada para a qual têm sido propostas orientações. Vallor, S. (2018), An Introduction to Cybersecurity Ethics, disponível em https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf [último acesso em13/09/2023].

contrário do que sucede nas medidas de gestão de riscos e nas obrigações de notificação e comunicação, nas medidas de supervisão e de execução a diretiva estabelece regimes jurídicos distintos para as entidades essenciais e para as entidades importantes.

As medidas de supervisão consistem em medidas de fiscalização. Para as entidades essenciais estão previstas no artigo 32.º e consistem, entre outras, em inspeções no local e supervisão remota, auditorias de segurança regulares e específicas, auditorias *ad hoc*, verificações de segurança conforme avaliação de riscos, pedidos de informação para avaliação das medidas de gestão de riscos, pedidos de acesso a dados, documentos e informações para fins de supervisão e pedidos de prova da aplicação de políticas de cibersegurança (artigo 32.º, n.º 2). O regime de supervisão mínimo previsto é mais rígido para as entidades essenciais. A título de exemplo, o artigo 32.º, n.º 2, alínea c) estabelece que as autoridades competentes dispõem de poderes para a realização de auditorias *ad hoc*, incluindo em casos justificados por um incidente significativo ou por infração à presente diretiva por parte da entidade essencial. Esta medida não possui paralelo no artigo 33.º, n.º 2, que apresenta o quadro mínimo de medidas de supervisão das entidades importantes. As entidades essenciais podem ser objeto de uma supervisão *ex ante*, com vista à prevenção de incidentes, ao passo que as entidades importantes são objeto apenas de supervisão *ex post* (após a ocorrência de um incidente). Uma exposição mais ampla e precisa com as diferenças entre as medidas de supervisão para entidades essenciais e importantes pode ser observada no Anexo 2.

Por outro lado, previstas no artigo 32.º, n.ºs 4 a 8 para as entidades essenciais, e no artigo 33.º, n.ºs 4 e 5 para as entidades importantes, as medidas de execução têm o objetivo de impedir ou corrigir um incidente ou corrigir deficiências ou infrações. Pretendem conduzir a entidade obrigada para um comportamento conforme com a diretiva, por exemplo através da adoção de instruções vinculativas ou de ordens para prevenir ou corrigir incidentes, ou até na aplicação de uma decisão dirigida à entidade abrangida (exceto às entidades da administração pública) que desrespeitou medidas adotadas e que suspende temporariamente uma certificação ou de uma autorização relativa a serviços prestados ou ou proibe temporariamente uma pessoa do exercício de funções de gestão ou representação legal nessa entidade, incluindo a aplicação de coimas (artigo 32.º, n.º 4 e n.º 5 e artigo 33.º, n.º 4).

Nas medidas executivas também ocorre a distinção de regimes jurídicos para entidades essenciais e importantes. Vejam-se dois exemplos. O primeiro está consubstanciado no artigo 32.º, n.º 4, al. g), segundo o qual, para as entidades essenciais, a autoridade competente pode designar um supervisor com funções bem definidas durante um determinado período para supervisionar o cumprimento dos artigos 21.º e 23.º. Esta intervenção não tem paralelo no artigo 33.º, n.º 4, da diretiva, relativo às entidades importantes. O segundo exemplo é a suspensão temporária de uma certificação ou autorização relativa a uma parte ou à totalidade dos serviços relevantes ou atividades da entidade e a proibição temporária do exercício de funções a pessoas singulares com responsabilidades de gestão a nível de diretor executivo ou de representante legal na entidade essencial, medidas que só têm lugar quando as medidas adotadas nos termos do artigo 32.º, n.º 4, alíneas a) a d) e f) se revelarem ineficazes (artigo 32.º, n.º 5). Para maiores detalhes, consultar os Anexos 3 e 4.

A função principal das medidas indicadas é a correção do comportamento que infringe a diretiva. Traduzindo-se numa interferência sobre a atividade das entidades abrangidas, o artigo 32.º, n.º 7 (aplicável também às entidades importantes ex vi artigo 33.º, n.º 5)

impõe a observância de parâmetros de orientação para as autoridades competentes. Ao decidirem as medidas executivas a aplicar, as autoridades competentes devem ter em consideração a gravidade da infração, duração da infração, antecedentes, danos causados, a intenção do agente, dentre outros. Neste ponto, importa esclarecer que a referência à intenção do agente como um dos elementos que deve modelar a aplicação das medidas executivas não significa a opção por um regime de responsabilização baseado na culpa. Os artigos 32.º, n.º 6 e 33.º, n.º 5 da diretiva não deixam dúvidas: a mera inobservância do dever de assegurar o cumprimento do regime imposto pela diretiva, independentemente de um eventual juízo de censura, é suficiente para a responsabilização de qualquer pessoa singular responsável por uma entidade essencial ou importante, que a represente legalmente, que tome decisões em seu nome ou que exerça seu controle.

O artigo 32.º, n.º 8 (aplicável também às entidades importantes ex vi artigo 33.º, n.º 5) determina que a aplicação das medidas de execução depende de prévia notificação com conclusões preliminares, da concessão de prazo razoável para pronúncia e da fundamentação pormenorizada da decisão.

Em suma, conclui-se que as medidas executivas devem ser aplicadas com respeito pelo princípio da proporcionalidade e com a observância de garantias processuais, como o direito de defesa, o direito ao contraditório e o direito a uma decisão fundamentada. Não obstante, o próprio artigo 32.º, n.º 8 da diretiva autoriza que em casos devidamente fundamentados sejam adotadas medidas executivas imediatas para prevenir ou responder a incidentes; nestas hipóteses, o direito ao contraditório é diferido para momento posterior à aplicação das medidas.

4.4. SANÇÕES

No quadro jurídico apresentado pela diretiva quanto às sanções, a distinção de tratamento entre entidades essenciais e importantes é meramente quantitativa. As sanções são sempre complementares das medidas de execução (artigo 34.º, n.º 2).

As entidades essenciais, caso violem as obrigações previstas nos artigos 21.º e 23.º, ficam sujeitas a coimas em montante máximo não inferior a 10 000 000 EUR ou num montante máximo não inferior a 2 % do volume de negócios anual a nível mundial, no exercício financeiro anterior, da empresa a que a entidade essencial pertence, consoante o montante que for mais elevado (artigo 34.º, n.º 4). Por outro lado, as entidades importantes, caso violem as obrigações previstas nos artigos 21.º e 23.º, ficam sujeitas a coimas em montante máximo não inferior a 7 000 000 EUR ou num montante máximo não inferior a 1,4 % do volume de negócios anual a nível mundial, no exercício financeiro anterior, da empresa a que a entidade importante pertence, consoante o montante que for mais elevado (artigo 34.º, n.º 5). De acordo com o regime previsto na diretiva, cabe aos Estados-membros definirem os montantes mínimos das coimas sancionatórias.

Ademais, nada impede os Estados-Membros de definirem montantes máximos superiores aos apontados na diretiva e de instituírem um quadro jurídico nacional mais amplo de sanções, incluindo sanções de natureza civil, administrativa, penal e sanções pecuniárias compulsórias. Os EM têm uma significativa margem de apreciação no recorte desse regime sancionatório, incluindo as medidas necessárias para a respetiva aplicação, mas sempre sujeitos à obrigação de instituírem sanções efetivas, proporcionadas e dissuasivas, tendo

em consideração as circunstâncias de cada caso concreto (artigo 34.º, n.º 1). Na respetiva aplicação devem ter em conta os parâmetros previstos no artigo 32.º, n.º 7, ex vi artigo 34.º, n.º 3. Os EM devem notificar a Comissão Europeia, até 17/01/2025, acerca dessas regras e medidas e de quaisquer alterações ulteriores (artigo 36.º).

5. A PROMOÇÃO DE UM CIBERESPAÇO SEGURO ALARGADO E MULTINÍVEL

Além dos quatro eixos principais anteriormente referidos, a Diretiva (UE) 2022/2555 revela um caráter inclusivo, através da partilha de informações e notificação voluntárias.

Por uma banda, a Diretiva 2022/2555 promove um espaço de cibersegurança alargado através do reconhecimento da colaboração de entidades não incluídas no seu âmbito de aplicação obrigatória. Entidades não obrigadas pela diretiva podem, a título voluntário, proceder ao intercâmbio de informações pertinentes sobre cibersegurança, nomeadamente relacionadas com ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques, tal como dispõe o artigo 29.º, n.º 1, als. a) e b). Do mesmo modo, segundo o artigo 30.º, nº 1, als. a) e b), entidades não obrigadas pela diretiva podem realizar notificações voluntárias às CSIRT ou, se aplicável, às autoridades competentes, em caso de incidentes significativos, ciberameaças e quase incidentes. Assim, há uma abertura inclusiva que permite a pequenas empresas não obrigadas pelas obrigações previstas na Diretiva a colaboração no reforço do nível de cibersegurança na União Europeia. Esta é ainda uma via para incrementar a sensibilização da sociedade sobre o tema, sem a qual não é possível a criação de um ambiente cibernético seguro.

No mesmo sentido, reconhece-se que não é possível a gestão de riscos em cibersegurança sem a promoção do conhecimento, sensibilização e desenvolvimento de competências na sociedade em geral. Como tal, destaca-se a preocupação da diretiva com o desenvolvimento de conhecimentos e competências em cibersegurança em toda a sociedade, elegendo esta preocupação como como parte necessária da estratégia nacional de cibersegurança (artigo 7.º, n.º 2, alínea f)), bem como a realização de ações de formação, no âmbito das entidades essenciais e importantes, para aquisição de conhecimentos e competências específicos necessários a uma boa gestão dos riscos de cibersegurança no contexto das atividades desempenhadas por cada entidade, seus dirigentes e colaboradores (artigo 20.º, n.º 2).

O quadro institucional de governação assenta no princípio “one-stop control”. As entidades obrigadas ficam sob a jurisdição do EM onde se encontrem estabelecidas (artigo 26., n.º 1), mas são significativas as exceções. Para os fornecedores de redes públicas de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público a competência é do EM em que prestam os serviços – al. a); para os prestadores de serviços de DNS, os registos de nomes de TLD, as entidades que prestam serviços de registo de nomes de domínio, os prestadores de serviços de computação em nuvem, os prestadores de serviços de centro de dados, os fornecedores de redes de

distribuição de conteúdos, os prestadores de serviços geridos, os prestadores de serviços de segurança geridos, bem como os prestadores de serviços de mercados em linha, de motores de pesquisa em linha ou de plataformas de serviços de redes sociais, a competência é do EM onde têm o seu estabelecimento principal, tal como determinado pelo n.º 2 ex vi al.b do n.º 1; e, as entidades da Administração Pública ficam sob a jurisdição do EM que as estabeleceu – al. c).

A efetiva aplicação da diretiva demanda uma atuação coordenada entre as autoridades competentes, tanto entre as autoridades do mesmo Estado-membro quanto entre autoridades de Estados-membros diferentes no âmbito da União, e ainda com as autoridades competentes setoriais previstas em outras diretivas, como a Diretiva (UE) 2022/2556 e a Diretiva (UE) 2022/2557. A necessidade desta atuação transversal e coordenada manifesta-se nas disposições que determinam a aplicação da diretiva sem prejuízo do Regulamento (UE) 2016/679, da Diretiva 2002/58/CE, das Diretivas 2011/93/UE e 2013/40/UE do Parlamento Europeu e do Conselho e da Diretiva (UE) 2022/2557 (artigo 2.º, n.º 12; artigo 32.º, n.º 9 e n.º 10; artigo 35.º). Segundo o artigo 9.º, "os Estados-Membros devem designar ou criar uma ou várias autoridades competentes responsáveis pela gestão de crises e de incidentes de cibersegurança em grande escala (autoridades de gestão de cibercrises)" e garantir "que essas autoridades dispõem dos recursos necessários para desempenhar, de forma eficaz e eficiente, as suas funções". É interessante observar que este caráter cooperativo e inclusivo é transversal e transnacional e está presente, entre outros, no estabelecimento de pontos de contacto únicos (artigo 8.º, n.º 4), na criação do Grupo de cooperação (artigo 14.º) e assistência mútua (artigo 37.º), tratamento de incidentes transfronteiriços (artigo 23.º, n.º 1, § 3).

No modelo preconizado, as CSIRT envolvem as autoridades competentes e os *stakeholders* privados dos setores abrangidos, seja para troca de informação, alertas, exercícios em matéria de ciberameaças e de incidentes, resposta a incidentes, gestão de crises e partilha de boas práticas, num regime inspirado nas parcerias público-privadas (PPP) que se projeta igualmente no nível europeu (artigos 10.º a 13.º e 15.º). Já a EU-CyCLONe constitui uma rede de cooperação entre as autoridades nacionais responsáveis pela gestão de crises cibernéticas e permite uma cooperação coordenada que responda adequadamente na gestão de crises de cibersegurança de grande dimensão, além de estabelecer a ligação entre o nível técnico, desempenhado pela rede de CSIRT e a gestão política das crises, tendo a ENISA o lugar central (artigo 16.º). Trata-se de um verdadeiro quadro de governação multinível, incluindo a avaliação por pares (artigo 19.º), e que prevê a possibilidade de participação em quadros de cooperação internacional com Estados terceiros ou organizações internacionais (artigo 17.º).

6. O IMPACTO DA DIRETIVA 2022/2555 NA LEGISLAÇÃO PORTUGUESA

O quadro normativo português da cibersegurança é constituído por diversos atos. A Lei n.º 46/2018 estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148 para o ordenamento jurídico português; o Decreto-Lei n.º 65/2021 regulamenta o referido regime jurídico, estabelecendo, em especial, obrigações em matéria de requisitos de segurança, certificação de cibersegurança e notificação de incidentes; o Regulamento n.º 183/2022, por fim, configura a instrução técnica relativa a

comunicações entre as entidades obrigadas pela legislação portuguesa e o Centro Nacional de Cibersegurança.

A adoção da Diretiva 2022/2555 implicará a adoção de medidas nacionais de transposição que modificarão os atos normativos mencionados. Evidentemente, nos estritos limites deste trabalho não é possível propor todas as alterações legislativas necessárias em razão da Diretiva (UE) 2022/2555, nem proceder a um grau elevado de pormenorização. Busca-se, antes, apresentar um panorama da legislação portuguesa e algumas perspetivas que nos parecem relevantes para as principais modificações indispensáveis aquando da transposição da nova diretiva.

6.1. O ÂMBITO SUBJETIVO DE APLICAÇÃO

A Lei n.º 46/2018 (bem como o Decreto-lei n.º 65/2021) reproduz a classificação adotada pela SRI1 e pela Diretiva 2008/114/CE. A nova diretiva aplica-se a novas entidades e divide-as em novas categorias: entidades essenciais e entidades importantes. Em consequência, o legislador português terá de alargar o âmbito de entidades abrangidas, para incluir os novos setores e subsetores indicados nos Anexos I e II da Diretiva 2022/2555 (v.g. o espaço; no setor da energia, o hidrogéneo; as águas residuais; os serviços postais e de estafeta; a produção, fabrico e distribuição de produtos químicos; a produção, transformação e distribuição de produtos alimentares; a indústria transformadora). Deverá igualmente adaptar a respetiva classificação em conformidade com a diretiva. Ainda assim, é de salientar que a legislação portuguesa já é aplicável à Administração Pública (artigo 2.º, n.º 1 da Lei n.º 46/2018), o que não era exigível à luz da Diretiva SRI1. Neste ponto já se verifica a conformidade com o regime da nova diretiva e a legislação portuguesa vai até além da previsão da Diretiva, pois incluem-se entre as entidades da Administração Pública abrangidas, não apenas a administração central, mas igualmente as regiões autónomas, as autarquias locais (que a Diretiva não inclui em termos obrigatórios), as entidades administrativas independentes, os institutos públicos, as empresas públicas e as associações públicas.

Por outro lado, estão excluídos da sua aplicação as redes e sistemas de informação diretamente relacionados com o comando e controlo do Estado-Maior-General das Forças Armadas e dos ramos das Forças Armadas e as redes e sistemas de informação que processem informação classificada (artigo 2.º, n.º 6). Nesse aspeto, portanto, a lei nacional compatibiliza-se com o artigo 2.º, n.ºs 5, 7 e 8 da SRI2. Convém observar, porém, que a definição de entidade da Administração Pública contida no artigo 3.º, ponto 35, da Diretiva "SRI 2" potencialmente extravasa e pode mesmo ser contraditória com o conceito subjacente ao artigo 2.º, n.º 2, da Lei nº 46/2018, pois os critérios materiais daquela não coincidem com o elenco formal do elenco desta última disposição.

6.2. AS MEDIDAS DE GESTÃO DE RISCOS DE CIBERSEGURANÇA

Conforme se pode observar, a Diretiva (UE) 2022/2555, em seus artigos 21.º e 24.º, cuida das medidas de gestão de riscos de cibersegurança, aplicáveis a entidades essenciais e importantes. Por sua vez, a Diretiva (UE) 2016/1148, nos seus artigos 14.º e 16.º, usava outras nomenclaturas: preferia a expressão "requisitos de segurança" para se referir às medidas de gestão de riscos a serem adotadas por "operadores de serviços essenciais"

(artigo 14.º, n.º 1 e n.º 2) e "prestadores de serviços digitais" (artigo 16.º, n.º 1 e n.º 2). Isto reflete-se, evidentemente, na legislação portuguesa adotada para a sua implementação. É por isso que os artigos 12.º, 14.º, 16.º e 18.º da Lei n.º 46/2018 cuidam da definição de requisitos de segurança (artigo 12.º) e dos respetivos requisitos para a Administração Pública e operadores de infraestruturas críticas (artigo 14.º), operadores de serviços essenciais (artigo 16.º) e prestadores de serviços digitais (artigo 18.º).

É necessário adaptar a legislação portuguesa às nomenclaturas adotadas pela atual diretiva: i) medidas de gestão de gestão de riscos de cibersegurança (artigo 21.º), o que inclui a utilização de sistemas europeus de certificação da cibersegurança (artigo 24.º), em lugar de requisitos de segurança; e, evidentemente, ii) referência às entidades essenciais e importantes em lugar da classificação resultante da diretiva anterior, tal como já referido.

A Lei n.º 46/2018 apresenta previsões específicas quanto aos requisitos de segurança, nos seus artigos 14.º, 16.º e 18.º, para cada tipo diferente de entidade abrangida. Daqui resulta uma diferenciação que desapareceu na atual diretiva, que, apesar de distinguir entidades essenciais e entidades importantes, não institui regimes jurídicos diferentes quanto às medidas de gestão de riscos para essas duas categorias. Uma das modificações legislativas a empreender será conformar a legislação portuguesa, nomeadamente as disposições referidas da Lei n.º 46/2018, com o regime da Diretiva "SRI 2". Se as categorias de entidades abrangidas deverão ser alteradas para se conformarem com as categorias previstas na nova Diretiva, já o regime mínimo das medidas de gestão de gestão de riscos de cibersegurança deverão ser uniformizadas, independentemente do tipo de entidade, sem prejuízo da possibilidade de adotar medidas mais exigentes, como admitido pelo artigo 5.º da Diretiva.

Não obstante, os maiores desenvolvimentos legislativos em Portugal quanto às medidas de gestão de riscos de cibersegurança (anteriormente designados como requisitos de segurança) resultam da regulamentação referida no artigo 31.º da Lei n.º 46/2018, e que se traduziu na elaboração do Decreto-Lei n.º 65/2021. Os artigos 7.º a 10.º do Decreto-Lei n.º 65/2021 instituem a obrigação de as entidades elaborarem um plano de segurança (artigo 7.º), apresentarem um relatório anual (artigo 8.º) e de instituírem e cumprirem medidas destinadas à gestão de riscos de cibersegurança após a devida análise desses riscos (artigos 9.º e 10.º).

As obrigações agora previstas são mais determinadas e exaustivas e constituem um verdadeiro "programa de governação corporativa e *compliance* em cibersegurança". Segundo a Diretiva (UE) 2022/2555, este programa deve observar conteúdos mínimos, como as obrigações de supervisão das medidas de gestão por parte dos órgãos de direção da entidade (artigo 20.º, n.º 1); ações de formação (artigo 20.º, n.º 2); e, sobretudo, as medidas propriamente ditas referidas no artigo 21.º, n.º 2, tendo em conta as vulnerabilidades e avaliações indicadas no artigo 21.º, n.º 3. O artigo 7.º do Decreto-Lei n.º 65/2021, ainda que já corresponda em certa medida às exigências da nova Diretiva (*v.g.* a nomeação de um responsável de segurança e também um ponto de contacto permanente ou a elaboração/atualização de um Plano de Segurança), é demasiado sucinto e fica aquém daquele conteúdo mínimo. Razões de certeza jurídica recomendam que a maior densificação do regime da Diretiva 2022/2555 seja refletida na legislação portuguesa, através da modificação do Decreto-Lei n.º 65/2021. Embora as medidas previstas no artigo 20.º, n.º 2 da diretiva se refiram à gestão de riscos de cibersegurança, estas não se limitam estritamente à análise de riscos – al. a); antes, alcançam matérias como o

tratamento de incidentes – al. b), continuidade das atividades – al. c), segurança da cadeia de abastecimento – al. d), segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação – al. e), avaliação da eficácia das medidas de gestão dos riscos de cibersegurança – al. f), práticas de ciber-higiene e formação – al. g), uso de criptografia e cifragem – al. h), segurança de recursos humanos e acesso e gestão de ativos – al. i), e, uso de soluções de autenticação e comunicações – al. j). Os artigos 9.º e 10.º do Decreto-Lei n.º 65/2021 parecem excessivamente focados na análise de riscos, sendo necessário também que a legislação portuguesa tenha atenção com a integralidade das medidas previstas no artigo 20.º, n.º 2, da Diretiva (UE) 2022/2555.

Por outro lado, o artigo 8.º do Decreto-Lei n.º 65/2021 prevê a elaboração de um relatório anual, o qual, embora não previsto expressamente na diretiva, constitui uma boa medida, consentânea com as obrigações fiscalizatórias do Estado-membro e facilitadora deste mister (artigo 20.º, n.º 1, da diretiva), sem prejuízo das obrigações de notificação e comunicação; além disso, está ao abrigo do artigo 5.º da diretiva.

6.3. AS OBRIGAÇÕES DE NOTIFICAÇÃO E COMUNICAÇÃO

A Diretiva (UE) 2022/2555, no seu artigo 23.º, n.º 1, estabelece obrigações de notificação de qualquer incidente que tenha um impacto significativo na prestação dos seus serviços, aplicáveis tanto a entidades essenciais quanto a entidades importantes, sem distinção de regime jurídico. Por sua vez, a Lei nº 46/2018 apresenta a matéria de maneira fragmentada, destacando-se o artigo 15.º para a notificação de incidentes para a Administração Pública e operadores de infraestruturas críticas, o artigo 17.º para a notificação de incidentes para os operadores de serviços essenciais e o artigo 19.º para a notificação de incidentes para os prestadores de serviços digitais. Assim como em relação às medidas de gestão de riscos, a ausência de distinção entre regimes jurídicos aplicáveis aos diferentes tipos de entidade indica que que as obrigações de notificação devem passar a ser tratadas na lei portuguesa de modo uniforme, e não fragmentado, pelo menos no que concerne ao regime de harmonização mínima. Sem prejuízo, o Estado português pode estabelecer obrigações de notificação adicionais, em conformidade com o artigo 5.º da diretiva, inclusive com obrigações específicas para os diferentes tipos de entidades.

Além disso, a Diretiva (UE) 2022/2555 utiliza outra expressão para o impacto dos incidentes que impõem a obrigação de notificação: em vez de impacto “relevante” ou “substancial”, prefere a expressão impacto “significativo”, expressão que parece acolher também impactos de alcance mais quantitativo e não apenas de tipo mais “qualitativo”. Será desejável que a legislação portuguesa acolha esta modificação.

Há que salientar que o regime vigente em Portugal já antecipa em alguma medida o novo regime europeu. Os artigos 15.º, 17.º e 19.º da Lei nº 46/2018 revelam elementos presentes também na Diretiva (UE) 2022/2555, tais como a importância do impacto transfronteiriço (artigo 23.º, n.º 1, § 3) e a não determinação de responsabilidades adicionais decorrentes do mero ato de notificação (artigo 23.º, n.º 1, § 1). Porém, nada se encontra, por exemplo, sobre impacto intersetorial significativo (artigo 23.º, n.º 1, § 3) e sobre as obrigações de comunicação aos destinatários dos serviços (artigo 23.º, n.º 1, § 1 e n.º 2), os quais deverão ser introduzidos no regime jurídico da segurança no ciberespaço português.

Cabe ainda destacar que, na esteira do já previsto na Diretiva (UE) 2016/1148, a Lei n.º 46/2018, no seu artigo 20.º, prevê a possibilidade de notificação voluntária de incidentes significativos por entidades não obrigadas pela diretiva, importante instrumento de inclusão também previsto na diretiva atual, conforme o artigo 30.º, n.º 1. Neste ponto, não é necessária uma modificação da legislação portuguesa, desde que feita a adaptação indispensável relativa às entidades obrigadas.

Os artigos 13.º e 31.º, n.º 2 da Lei n.º 46/2018 remetem para regulamentação complementar o regime das obrigações de notificação, o que se deu com os artigos 11.º a 17.º e 19.º do Decreto-Lei n.º 65/2021 e artigo 6.º do Regulamento n.º 183/2022. Quanto ao procedimento das obrigações de notificação, a Diretiva (UE) 2022/2555 dispõe, no seu artigo 23.º, n.º 4, sobre quatro tipos de atos: i) alerta rápido, em 24 horas após o conhecimento do incidente (artigo 23.º, n.º 4, al. a); ii) notificação de incidente, em 72 horas após o conhecimento do incidente (artigo 23.º, n.º 4, al. b); iii) relatório final, no mais tardar um mês após a notificação de incidente ou após a resolução do incidente, com conteúdo mínimo definido na diretiva (artigo 23.º, n.º 4, al. d); iv) relatório intercalar eventual, quando a CSIRT ou autoridade competente entender pela necessidade de prestação de informações atualizadas ou quando ao tempo da elaboração do relatório final o incidente ainda esteja em curso (artigo 23.º, n.º 4, als. c) e e)). Por sua vez, os artigos 12.º a 15.º do Decreto-Lei n.º 65/2021 estabelecem um procedimento de notificação inicial, 2 horas após a verificação do incidente; notificação de fim de impacto relevante ou substancial, 2 horas após a perda de impacto relevante ou substancial; e notificação final, 30 dias após o término do incidente. Há, portanto, algumas diferenças. É certo que a lei portuguesa deve adequar-se ao procedimento das obrigações de notificação e à nomenclatura utilizada pela Diretiva (UE) 2022/2555 (alerta rápido, notificação de incidente, relatório final e relatório intercalar). Contudo, quanto ao cumprimento dos prazos de notificação, a lei nacional atual é mais exigente e praticamente adota um regime de notificação em tempo real, com prazos bem menores do que aqueles descritos na diretiva; neste ponto, considerando o regime de harmonização mínima, o Estado português pode decidir manter esse regime de notificação praticamente em tempo real, sem qualquer contrariedade com a diretiva atual e contribuindo para um ciberespaço mais seguro.

O artigo 19.º do Decreto-Lei n.º 65/2021 e o artigo 6.º do Regulamento n.º 183/2022 fornecem informações práticas para a operacionalização do procedimento de notificação, relativas a seu formato e não se vislumbra qualquer incompatibilidade entre eles e a diretiva atual.

Por fim, os atos de execução relativos às obrigações de notificação e comunicação (artigo 23.º, n.º 11, § 1) e ao enquadramento do conceito de incidente significativo (artigo 23.º, n.º 11, § 2) quando adotados pela Comissão Europeia podem exigir novas medidas nacionais de tipo regulamentar.

6.4. AS MEDIDAS DE SUPERVISÃO E EXECUÇÃO

Quanto às medidas de supervisão e execução, os atos normativos portugueses são bastante escassos. Há apenas um artigo sobre o tema, que é o artigo 21.º da Lei nº 46/2018, segundo o qual “as competências de fiscalização e de aplicação das sanções previstas na presente lei cabem ao Centro Nacional de Cibersegurança”. Portanto, não há um quadro normativo nacional para as medidas de supervisão e execução.

Embora o Centro Nacional de Cibersegurança tenha o exercício da competência que lhe foi atribuída para a fiscalização e da aplicação de sanções em matéria de cibersegurança, tal não substitui a exigência de que a lei de transposição preveja um quadro de medidas de supervisão e execução.

É necessário, portanto, que se incluam na legislação portuguesa, no mínimo, o quadro de medidas e sua respectiva regulação, referidos sucintamente *supra*, alusivos aos artigos 31.º a 35.º da Diretiva (UE) 2022/2555, respeitando-se a diferença qualitativa entre os regimes jurídicos instituídos para entidades essenciais e para entidades importantes. Esta distinção qualitativa pode ser observada nos quadros anexos a este trabalho.

Sem prejuízo, o Estado português pode, à luz do que dispõe o artigo 5.º da diretiva, estabelecer outras medidas de supervisão e execução não previstas na diretiva, especialmente para as entidades essenciais, tendentes à elevação do nível de cibersegurança, desde que tais disposições sejam compatíveis com as obrigações dos Estados-membros decorrentes do direito da União.

6.5. SANÇÕES

Na legislação portuguesa, a matéria é tratada nos artigos 21.º a 28.º da Lei n.º 46/2018 e no artigo 21.º do Decreto-Lei n.º 65/2021. O artigo 28.º determina a aplicação subsidiária do regime geral das contraordenações.

Os artigos 21.º e 26.º da Lei n.º 46/2018 estabelecem que a aplicação de sanções e a instrução dos processos de contraordenação competem ao Centro Nacional de Cibersegurança. O produto das coimas aplicadas reverte em 60% para o Estado e 40% para o Centro Nacional de Cibersegurança (artigo 27.º).

Os artigos 23.º e 24.º estabelecem que as infrações muito graves e graves são puníveis com a aplicação de coimas, que variam, para infrações muito graves, entre € 5000 e € 25 000, tratando-se de uma pessoa singular, e entre € 10 000 e € 50 000, no caso de se tratar de uma pessoa coletiva; para infrações graves, as coimas variam entre € 1000 e € 3000, tratando-se de uma pessoa singular, e entre € 3000 e € 9000, no caso de se tratar de uma pessoa coletiva. O artigo 25.º prevê punição também em caso de negligência, com redução de metade.

Por outro lado, o artigo 21.º do Decreto-Lei n.º 65/2021 contém algumas disposições complementares sobre o regime sancionatório, bem como a previsão de outras infrações, igualmente puníveis com a aplicação de coimas entre € 1000 e € 3740,98, no caso de pessoa singular, ou entre € 5000 e 44 891,81, no caso de pessoa coletiva.

De maneira geral, a Diretiva (UE) 2022/2555 estabelece um conjunto de obrigações para os EM: i) a aplicação de coimas por violação aos artigos 21.º e 23.º, nos termos do artigo 34.º, n.º 4 e n.º 5, com uma distinção quantitativa entre os regimes aplicáveis a entidades essenciais e importantes e com valores mínimos para o montante máximo da medida da sanção expressamente determinados; ii) a observação dos princípios da efetividade e da proporcionalidade (artigo 34.º, n.º 1 e n.º 3); e, iii) a instituição de um quadro nacional de sanções e de medidas necessárias à sua aplicação, bem como o dever de notificar a Comissão Europeia, até 17/01/2025, acerca dessas regras e medidas e o dever de comunicar quaisquer alterações ulteriores (artigo 36.º). O Estado português está

autorizado a instituir um quadro jurídico nacional mais amplo de sanções do que o previsto na Diretiva, incluindo sanções de natureza civil, administrativa e penal (artigo 5.º da diretiva).

Do cotejo entre a Diretiva (UE) 2022/2555 e o regime sancionatório previsto na Lei n.º 46/2018 e no Decreto-Lei n.º 65/2021, observa-se a necessidade de inclusão, na lei portuguesa, de significativas modificações, para que seja respeitado o regime imperativo da diretiva.

É imediatamente evidente e imperioso que a legislação portuguesa tem de ser modificada para que cumpra o valor mínimo previsto na Diretiva para o montante máximo das coimas (cujos montantes são absolutamente díspares), com a distinção já referida quantitativa entre os regimes aplicáveis a entidades essenciais e importantes.

No que respeita às condições gerais para aplicação de coimas, impõe-se observação de princípios como efetividade e proporcionalidade (artigo 34.º, n.º 1) e de parâmetros como a gravidade da infração e a importância das disposições violadas, a duração da infração, quaisquer anteriores infrações relevantes cometidas pela entidade em causa, quaisquer danos materiais ou imateriais causado, os efeitos noutros serviços e o número de utilizadores afetados, qualquer intenção ou negligência do autor da infração, quaisquer medidas tomadas pela entidade para prevenir ou atenuar os danos materiais ou imateriais, qualquer cumprimento de códigos de conduta ou procedimentos de certificação aprovados e o nível de cooperação das pessoas singulares ou coletivas consideradas responsáveis com as autoridades competentes (artigo 34.º, n.º 3, conjugado com o artigo 32.º, n.º 7).

Conquanto alguns desses parâmetros já decorreriam genericamente da previsão de aplicação subsidiária do regime geral das contraordenações, nos termos do artigo 28.º da Lei n.º 46/2018 combinado com o artigo 18.º do Decreto-Lei n.º 433/1982,o regime geral das contraordenações, por si só, é manifestamente insuficiente para parametrizar a aplicação de sanções decorrentes de ofensa ao conteúdo da Diretiva (UE) 2022/2555. A diretiva instituiu um regime específico, com parâmetros próprios, e que por isso deve ser incluído na legislação específica da cibersegurança, prevalecendo de modo inequívoco sobre o regime geral das contraordenações, que poderá ser mantido como regime subsidiário. Para melhor compreensão das muitas diferenças entre os parâmetros para aplicação de coimas na Diretiva (UE) 2022/2555 e no Decreto-Lei n.º 433/1982, confira-se o Anexo n.º 5. Quanto ao mais, embora as infrações previstas na legislação não pareçam conflituar com a Diretiva (UE) 2022/2555, é salutar que o Estado português proceda a uma revisão do quadro jurídico de sanções, inclusive submetendo à sua própria decisão político-legislativa a conveniência da previsão de outras condutas puníveis e de outras sanções, de natureza cível, administrativa e criminal, em conformidade com o artigo 5.º da diretiva atual.

Por fim, uma vez realizada a transposição da diretiva e efetuada esta revisão do quadro de sanções, o Estado português deverá notificar a Comissão Europeia, até 17/01/2025, acerca das regras e medidas adotadas e de quaisquer alterações ulteriores, segundo o artigo 36.º da Diretiva (UE) 2022/2555.

7. CONSIDERAÇÕES CONCLUSIVAS

Como anteriormente afirmado, não foi escopo deste trabalho efetuar uma análise pormenorizada de todas as modificações necessárias na transposição da Diretiva (UE) 2022/2555 para o ordenamento jurídico português, mas, sim, a apresentação de um panorama sobre o regime jurídico instituído pela Diretiva (UE) 2022/2555 e o apontamento geral das principais modificações que se mostram como necessárias em face do novo regime, em relação às entidades obrigadas, às medidas de gestão de riscos, às obrigações de notificação e comunicação, às medidas de supervisão e execução e ao quadro jurídico de sanções.

Tudo isso, contudo, seria vazio sem um prévio périplo pela interação entre a cibersegurança, o Direito e os direitos e pelo quadro normativo e institucional da cibersegurança na UE e em Portugal. A compreensão desses elementos demonstra que o modelo adequado de regulação jurídica europeia da cibersegurança é um modelo de regulação multinível que seja apto para alcançar um ponto de equilíbrio entre flexibilidade, para atender à velocidade das transformações digitais, e a segurança jurídica de uma regulação vinculante; que seja capaz de se articular com os instrumentos de *soft law*, com destaque para os organismos de estandardização; que se articule com outros domínios associados; que reconheça seu caráter transfronteiriço; que promova a cooperação entre as autoridades competentes, a nível nacional e europeu; e que fomente a inclusão, educação e a sensibilização da sociedade para uma condução segura e responsável de seus comportamentos no meio digital.

A nova diretiva não tem um alcance revolucionário, mas o seu regime traduz uma evolução que reforça as exigências de cibersegurança para um conjunto bastante mais alargado de entidades, melhora as condições de supervisão e execução, reforça a responsabilização dos órgãos de gestão e o regime sancionatório. Reforça igualmente o quadro institucional e a cooperação multinível entre as autoridades nacionais e europeias competentes. Confirma-se a referida perspetiva holística assente no controlo do risco, com uma preocupação primordial na prevenção e secundária na minimização e mitigação dos danos.

É indubitável a conclusão de que o regime vigente em Portugal, ainda que seja conforme com a Diretiva revogada não é conforme com o novo regime da Diretiva 2022/2555 e são necessárias medidas em todas as dimensões: da gestão de riscos até ao quadro sancionatório.

Dito isto, a extensão e a profundidade das modificações promovidas pela Diretiva (UE) 2022/2555 indicam, em nossa opinião, a necessidade de elaboração de uma nova lei (ou um conjunto de leis) para regular o regime jurídico da cibersegurança em Portugal. Como no âmbito da União Europeia foi adotada uma nova diretiva para a cibersegurança, a melhor solução parece ser a elaboração de uma nova lei de transposição, e não apenas a alteração das leis já existentes. Este novo regime jurídico nacional deverá ser mais substancial. O aprofundamento no tratamento das matérias conferido pela nova diretiva conjugado com a diminuição da margem de apreciação antes permitida aos Estados-membros pela diretiva revogada aponta para a necessidade de um regime normativo mais denso do que o do quadro jurídico nacional ainda vigente.

O Estado português deverá implementar o conteúdo do quadro de harmonização mínima da Diretiva (UE) 2022/2555, modificando o âmbito subjetivo das entidades abrangidas de acordo com as novas classificações, reforçando e atualizando, incluindo a nomenclatura, as medidas de gestão de riscos, obrigações de notificação e comunicação, as diferenciadas medidas de supervisão e execução e o específico regime sancionatório. Além disso, deverá realizar suas próprias escolhas político-legislativas, na formação do quadro jurídico nacional, eventualmente indo além do regime mínimo imposto, considerando as especificidades da realidade portuguesa, de modo a garantir um elevado nível de cibersegurança, em conformidade com o artigo 5º da diretiva.

Mais em concreto, parece apropriada uma abordagem uniforme para o quadro mínimo comum de medidas de gestão de risco em lugar de uma abordagem fragmentada por tipo de entidade. A ausência de regimes jurídicos diferentes para entidades essenciais e importantes neste campo justifica esta opção. O Estado português deverá, ainda, exigir um programa de governança corporativa e *compliance* em cibersegurança para as entidades obrigadas, ainda que sob a atual denominação de "plano de segurança", adequando seu conteúdo às exigências mínimas da diretiva. Poderá manter, segundo sua margem de apreciação, a exigência o relatório anual a que se refere o artigo 8.º do Decreto-Lei n.º 65/2021. Deverá ampliar as exigências dos artigos 9.º e 10.º do Decreto-Lei n.º 65/2021 para que não estejam excessivamente focados na análise de riscos, mas incluam a globalidade das medidas previstas no artigo 20.º, n.º 2, da Diretiva (UE) 2022/2555.

Por outro lado, deve avaliar-se a oportunidade e conveniência, no âmbito da liberdade conferida pelo artigo 5.º, do estabelecimento de determinadas medidas de gestão adicionais, não previstas na diretiva, para as entidades abrangidas, especialmente para as essenciais, bem como decidir se as entidades abrangidas pela diretiva deverão ou não estar obrigadas a utilizar determinados produtos de TIC, serviços de TIC e processos de TIC certificados no âmbito de sistemas europeus de certificação da cibersegurança, para fins de cumprimento das medidas de gestão de riscos (artigo 24º).

No que respeita às obrigações de notificação, a legislação portuguesa deverá refletir as nomenclaturas adotadas pela nova diretiva; além disso, também aqui parece mais apropriada uma abordagem legal uniforme, e não fragmentada por tipo de entidade, em decorrência da ausência de distinção entre regimes jurídicos aplicáveis a entidades essenciais e importantes, pelo menos no âmbito do regime de harmonização mínima. O Estado português poderá estabelecer obrigações de notificação adicionais, em conformidade com o artigo 5.º da diretiva, inclusive com obrigações específicas para os diferentes tipos de entidades. Nas obrigações de comunicação, as obrigações relativas aos incidentes com impacto sectorial significativo (artigo 23.º, n.º 1, § 3) e as obrigações de comunicação aos destinatários dos serviços (artigo 23.º, n.º 1, § 1 e n.º 2) deverão ser introduzidos no futuro regime português.

Em relação ao procedimento de notificação de incidentes, a lei portuguesa prevê uma obrigação de notificação inicial que é temporalmente mais exigente (até 2 horas) do que o alerta rápido (até 24 horas); não obstante, são indispensáveis adaptações no que toca aos termos da obrigação de notificação de incidente e ao relatório final.

Quanto às medidas de supervisão e execução, a ausência de um quadro normativo nacional impõe que seja introduzido na legislação portuguesa, pelo menos, o quadro de medidas e sua respetiva regulação alusivos aos artigos 31.º a 35.º da Diretiva (UE) 2022/2555, respeitando-se a diferença qualitativa entre os regimes jurídicos instituídos

para entidades essenciais e para entidades importantes. Deve também ser avaliado o estabelecimento de outras medidas de supervisão e execução não previstas na diretiva, segundo autoriza seu artigo 5.º.

No que se refere ao regime sancionatório, as medidas de implementação serão exigentes. Desde logo, não poderá manter-se como critério principal da diferenciação das coimas a natureza individual ou coletiva do agente, mas antes a natureza essencial ou importante da entidade em causa. Em segundo lugar, o quadro vigente não corresponde às exigências da diretiva de efetividade e proporcionalidade. Em especial, a medida das sanções deverá respeitar os limiares diferenciados determinados pela diretiva para a medida superior das sanções (artigo 34.º, n.º 4 e 5) para as entidades essenciais e importantes, sem prejuízo de poder estabelecer valores superiores aos definidos na diretiva. No que concerne aos limiares mínimos, os valores da legislação portuguesa vigente deverão ser aumentados para que as sanções sejam efetivas e dissuasoras.

Deverá, igualmente, ser avaliada a conveniência da previsão de outras condutas puníveis e de outras sanções, de natureza cível, administrativa e criminal, no quadro da liberdade conferida pelo artigo 5.º. A mera previsão atual de aplicação subsidiária do regime geral das contraordenações, consoante o artigo 28.º da Lei n.º 46/2018 combinado com o artigo 18.º do Decreto-Lei n.º 433/1982, é claramente insuficiente para cumprir esta finalidade.

Uma vez instituído o novo quadro nacional de sanções, o Estado português deverá notificar a Comissão Europeia, até 17/01/2025, acerca das regras e medidas adotadas e de quaisquer alterações ulteriores, segundo o artigo 36.º da Diretiva (UE) 2022/2555.

Ademais, o legislador português deve promover a participação da sociedade e de entidades não obrigadas pela diretiva, por meio de ações educativas, de formação, e do uso dos institutos de notificação voluntária e partilha voluntária de informações.

É igualmente importante assegurar uma coordenação virtuosa entre as autoridades competentes, no nível nacional e supranacional, previstas na Diretiva (UE) 2022/2555 ou em instrumentos normativos conexos. Uma atenção especial deve ser dada às competências e meios do Centro Nacional de Cibersegurança e será necessário revisitar a respetiva orgânica e competências. Só esta abordagem será apta a construir um ciberespaço seguro e um quadro normativo e institucional apropriado à rápida transformação digital e aos intercâmbios transfronteiriços e intersetoriais tão próprios desta matéria.

Referências Bibliográficas

Barbosa Caseiro, I. (2022). *A Segurança do Ciberespaço Europeu.* Disponível em: https://eurodefense.pt/wp-content/uploads/2022/11/02_A-Seguran%C3%A7a-do-Ciberespa%C3%A7o-Europeu-13OUT2021.pdf.

Choucri, N. (2015). *Explorations in Cyber International Relations. A Research Collaboration of MIT and Harvard University. The Final Report Version 1.2*, Cambridge: Mass. Disponível em: https://ecir.mit.edu/final-report.

CNCS (2020). *Relatório Cibersegurança em Portugal: Ética & Direito*. Lisboa: Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/relatorio-eticadireito2020-observatoriociberseguranca-cncs.pdf.

CNCS (2021). *Relatório Cibersegurança em Portugal: Políticas Públicas*. Lisboa: Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/relatorio-politicaspublicas2021-observatoriociberseguranca-cncs.pdf.

Eggenschwiler, J. (2019), *International Cybersecurity Norm Development: The Roles of States Post-2017.* EU Cyber Direct.

Enes, G. (2021). A União Europeia Digital. Uma governação multinível ao serviço das pessoas, *E.TEC Yearbook. Governance & Technology*, UMinho, 115-138.

ENISA (2023). *Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies.* Disponível em: https://www.enisa.europa.eu/publications/building-effective-governance-frameworks-for-the-implementation-of-national-cybersecurity-strategies/@@download/fullReport.

ENISA (2023). *Developing National Vulnerabilities Programmes.* Disponível em: https://www.enisa.europa.eu/publications/developing-national-vulnerabilities-programmes/@@download/fullReport.

ENISA (2020). *National Capabilities Assessment Framework.* Disponível em: https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework/@@download/fullReport.

ENISA (2021). *Raising Awareness of Cybersecurity. A key element of national cybersecurity strategies.* Disponível em: https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity/@@download/fullReport.

European Commission (2021). *Communication Better Regulation: Joining forces to make better laws.* Disponível em: https://commission.europa.eu/system/files/2021-04/better_regulation_joining_forces_to_make_better_laws_en_0.pdf.

European Commission (2021). *Better Regulation Toolbox.* Disponível em: https://commission.europa.eu/system/files/2023-02/br_toolbox-nov_2021_en.pdf.

European Commission (2021). *Staff Working Document: Better Regulation Guidelines.* Disponível em: https://commission.europa.eu/system/files/2021-11/swd2021_305_en.pdf.

Macák, K. (2016). Is the international law of cybersecurity in crisis?, In N.Pissanidis et al. (eds.), *Cyber Power: 2016 8th International Conference on Cyber Conflict*, NATO Publications, 127-139.

Ministério dos Negócios Estrangeiros (2014). *Manual de Boas Práticas para a Negociação, Transposição e Aplicação de Legislação da União Europeia.* Disponível em: https://www.historico.portugal.gov.pt/download.ashx?media=/media/1538024/Manual%20DGAE%20Transposi%C3%A7%C3%A3o%20de%20diretivas.pdf

Observatório de Cibersegurança do CNCS (2020). *Cibersegurança em Portugal Ética & Direito.* Disponível em: https://www.cncs.gov.pt/docs/relatorio-eticadireito2020-observatoriociberseguranca-cncs.pdf.

Observatório de Cibersegurança do CNCS (2021). *Relatório sobre as Políticas Públicas de Cibersegurança.* Disponível em: https://www.cncs.gov.pt/docs/relatorio-politicaspublicas2021-observatoriociberseguranca-cncs.pdf.
OECD (2022). *Better Regulation Practices across the European Union 2022.* Disponível em: https://read.oecd.org/10.1787/6e4b095d-en?format=pdf.
Osula, A-M & Rõigas, H. (2016). *International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO Publications.
Papakonstantinou, V. (2022). The Cybersecurity Obligations of States Perceived as Platforms: Are Current European National Cybersecurity Strategies Enough?, *Applied Cybersecurity & Internet Governance*, *1*(1), DOI: 10.5604/01.3001.0016.1237.
Pernice, I. (2017). Cybersecurity governance: Making cyberspace a safer place. *HIIG Discussion Paper Series*, *2017*(05). Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=30121.
Pernik, P. (2022). Drivers of Change Impacting Cyberspace in 2030, In P. Pernik (Ed.), *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, 59, 56-79. Disponível em: https://ccdcoe.org/uploads/2022/03/Horizon_Scanning_v2_170x240_220513.pdf.
Ramos, M.E. (2021) Corporate governance and cyber governance. How to govern the future?, *E.TEC Yearbook. Governance & Technology*, UMinho, 157 – 178.
Santos, L., & Marques Guedes, A. (2015). Breves reflexões sobre Poder e Ciberespaço. *RDeS–Revista de Direito e Segurança, 6*(2015), 189-209. Disponível em https://comum.rcaap.pt/bitstream/10400.26/14329/1/PodereCiberesa%C3%A7o.pdf
Schmitt, M.N. (2017). Grey Zones in the International Law of Cyberspace. *The Yale Journal of International Law*, *42*(2), 1-21. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3180687#.
Shears, M., Shnidrig, D. & Kaspar, L. (2018). *Multistakeholder Approaches to National Cybersecurity Strategy Development.* Global Partners Digital. Disponível em: https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf.
Sliwinski, K.F. (2014). Moving beyond the European Union's Weakness as a Cyber-Security Agent, *Contemporary Security Policy, 35*(3), 468-486, DOI: 10. 1080/ 13523260. 2014. 959261.
Sousa Guedes, I. & Gomes, M.A. (2021). *Cibercriminalidade: novos desafios, ofensas e soluções*, Pactor, ISBN: 9789896931223.
Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication, 63*(3), 382-412.
Štrucl, D. (2021). *Comparative study on the cyber defence of NATO Member States.* NATO Cooperative Cuber Defence Centre of Excellence. Disponível em: https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf.
Vallor, S. (2018), *An Introduction to Cybersecurity Ethics.* Disponível em https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf. Acesso em 13/09/2023.
Vandezande, N. (2023). *Cybersecurity in the EU: How the Nis2-Directive Stacks Up Against its Predecessor*. Disponível em: https://ssrn.com/abstract=4383118 ou http://dx.doi.org/10.2139/ssrn.4383118.
World Economic Forum (2022). *Global Cybersecurity Outlook 2022.* Disponível em: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

Referências Normativas

Declaração Europeia sobre os direitos e princípios digitais para a década digital. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32023C0123(01)

Diretiva 2008/114/CE, de 08 de dezembro de 2008. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32008L0114.

Diretiva (UE) 2013/36, de 26 de junho de 2013. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:176:0338:0436:Pt:PDF.

Diretiva (UE) 2016/1148, de 06 de julho de 2016. Disponível em: https://eur-lex.europa.eu/eli/dir/2016/1148/oj?locale=pt.

Diretiva (UE) 2022/2555, de 14 de dezembro de 2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022L2555.

Diretiva (UE) 2022/2557, de 14 de dezembro de 2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022L2557.

Decreto-Lei n.º 65/2021, de 30 de julho de 2021. Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988.

Decreto-Lei n.º 20/2022, de 28 de janeiro de 2022. Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/20-2022-178264070.

Lei n.º 46/2018, de 13 de agosto de 2018. Disponível em: https://www.policiajudiciaria.pt/lei-n-o-46-2018-de-13-agosto/#:~:text=Sum%C3%A1rio%3A,informa%C3%A7%C3%A3o%20em%20toda%20a%20Uni%C3%A3o.

Recomendação 2003/361/CE da Comissão Europeia, de 06 de maio de 2003. Disponível em: https://eur-lex.europa.eu/eli/reco/2003/361/oj.

Regulamento (UE) 2022/2554, de 14 de dezembro de 2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2554.

Resolução do Conselho de Ministros n.º 92/2019. *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Disponível em https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/92-2019-122498962

Anexos

ANEXO 1: ENTIDADES ABRANGIDAS QUADRO I NOVAS ENTIDADES NO ÂMBITO DA SRI2		
1) Entidades essenciais		**Fundamento**
1.1	Produtores de energia elétrica na aceção do artigo 2º, ponto 38, da Diretiva (UE) 2019/944	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.2	Operadores nomeados do mercado da eletricidade na aceção do artigo 2º, ponto 8, do Regulamento (UE) 2019/943 do Parlamento Europeu e do Conselho	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.3	Participantes no mercado na aceção do artigo 2º, ponto 25, do Regulamento (UE) 2019/943, que prestam serviços de agregação, resposta da procura ou armazenamento de energia na aceção do artigo 2º, pontos 18, 20 e 59, da Diretiva (UE) 2019/944	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.4	Os operadores de um ponto de carregamento que são responsáveis pela gestão e operação de um ponto de carregamento que presta um serviço de carregamento aos utilizadores finais, incluindo em nome e por conta de um prestador de serviços de mobilidade, **que excedam os limiares para as médias empresas previstos no artigo 2º, nº 1, do anexo da Recomendação 2003/361/CE**	Não é entidade crítica nos termos da Diretiva 2022/2557 e, portanto, submete-se à regra geral do art. 3º., n. 1, a), da Diretiva 2022/2555.
1.5	Operadores de aquecimento urbano ou de arrefecimento urbano na aceção do artigo 2º, ponto 19, da Diretiva (UE) 2018/2001 do Parlamento Europeu e do Conselho	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.6	Entidades centrais de armazenagem de petróleo na aceção do artigo 2º, alínea f), da Diretiva 2009/119/CE do Conselho	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.7	Operadores de produção, armazenamento e transporte de hidrogénio	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.8	Operadores de serviços públicos de transporte na aceção do artigo 2º, alínea d), do Regulamento (CE) nº 1370/2007 do Parlamento Europeu e do Conselho	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557

1.9	Laboratórios de referência da UE na aceção do artigo 15º do Regulamento (UE) 2022/2371 do Parlamento Europeu e do Conselho	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.10	Entidades que realizam atividades de investigação e desenvolvimento de medicamentos na aceção do artigo 1º, ponto 2, da Diretiva 2001/83//CE do Parlamento Europeu e do Conselho	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.11	Entidades que fabricam produtos farmacêuticos de base e preparações farmacêuticas a que se refere a secção C, divisão 21, da NACE Rev. 2	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.12	Entidades que fabricam dispositivos médicos considerados críticos durante uma emergência de saúde pública («lista de dispositivos críticos para a emergência de saúde pública») na aceção do artigo 22º do Regulamento (UE) 2022/123 do Parlamento Europeu e do Conselho	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.13	Entidades titulares de uma autorização de distribuição a que se refere o artigo 79º da Diretiva 2001/83/CE	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.14	Empresas que recolhem, eliminam ou tratam águas residuais urbanas, águas residuais domésticas ou águas residuais industriais na aceção do artigo 2º, pontos 1, 2 e 3, da Diretiva 91/271/CEE do Conselho, com exceção das empresas nas quais a recolha, eliminação ou tratamento de águas residuais urbanas, águas residuais domésticas e águas residuais industriais constitui uma parte não essencial da sua atividade geral	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.15	Prestadores de serviços de centro de dados na aceção do artigo 6º, ponto 31, da Diretiva (UE) 2022/2555	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.16	Fornecedores de redes de distribuição de conteúdos na aceção do artigo 6, ponto 32, da Diretiva (UE) 2022/2555	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.17	Prestadores de serviços de confiança na aceção do artigo 3º, ponto 19, do Regulamento (UE) nº 910/2014 do Parlamento Europeu e do Conselho	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557

1.18	Fornecedores de redes públicas de comunicações eletrónicas na aceção do artigo 2º ponto 8, da Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.19	Fornecedores de serviços de comunicações eletrónicas na aceção do artigo 2.o, ponto 4, da Diretiva (UE) 2018/1972, na medida em que os seus serviços sejam acessíveis ao público	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.20	Entidades da administração pública a nível central tal como definidas pelos Estados-Membros em conformidade com o direito nacional	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557
1.21	Operadores de infraestruturas terrestres detidas, geridas e operadas pelos Estados-Membros ou por entidades privadas que apoiam a oferta de serviços espaciais, excluindo os fornecedores de redes públicas de comunicações eletrónicas na aceção do artigo 2º, ponto 8, da Diretiva (UE) 2018/1972	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557.
1.22	Prestadores de serviços geridos (TIC), **que excedam os limiares para as médias empresas previstos no artigo 2º, nº 1, do anexo da Recomendação 2003/361/CE**	Não é entidade crítica nos termos da Diretiva 2022/2557 e, portanto, submete-se à regra geral do art. 3º., n. 1, a), da Diretiva 2022/2555.
1.23	Prestadores de serviços de segurança geridos (TIC), **que excedam os limiares para as médias empresas previstos no artigo 2º, nº 1, do anexo da Recomendação 2003/361/CE**	Não é entidade crítica nos termos da. Diretiva 2022/2557 e, portanto, submete-se à regra geral do art. 3º., n. 1, a), da Diretiva 2022/2555.
1.24	Empresas do setor alimentar na aceção do artigo 3º., ponto 2, do Regulamento (CE) nº. 178/2002 do Parlamento Europeu e do Conselho, que estejam envolvidas **exclusivamente na logística** e na distribuição por grosso e produção e transformação industriais **em grande escala**	Diretiva 2022/2555, art. 2º., n. 3 c/c art. 3º., n. 1, f) - entidade crítica nos termos da Diretiva 2022/2557.
1.25	Empresas do setor alimentar, na aceção do artigo 3º, ponto 2, do Regulamento (CE) nº. 178/2002 do Parlamento Europeu e do Conselho (3), que se dedicam à distribuição por grosso e à produção e transformação industriais, **que excedam os limiares para as médias empresas previstos no artigo 2º, nº 1, do anexo da Recomendação 2003/361/CE**	Diretiva 2022/2555, art. 3º., n. 1, a). Diversamente do item 1.24, esta hipótese do anexo II da Diretiva 2022/2555 não abrange as expressões "exclusivamente na logística" e "em grande escala".

2) Entidades importantes		
2.1	Prestadores de serviços postais na aceção do artigo 2º, ponto 1-A, da Diretiva 97/67/CE, incluindo prestadores de serviços de estafeta	Diretiva 2022/2555, art. 3º., n. 2.
2.2	Empresas que realizam a gestão de resíduos na aceção do artigo 3º, ponto 9, da Diretiva 2008/98/CE do Parlamento Europeu e do Conselho, mas excluindo as empresas para as quais a gestão de resíduos não constitui a atividade económica principal	Diretiva 2022/2555, art. 3º., n. 2.
2.3	Empresas que realizam a produção de substâncias e a distribuição de substâncias ou misturas, referidas no artigo 3º, pontos 9 e 14, do Regulamento (CE) nº 1907/2006 do Parlamento Europeu e do Conselho e empresas que realizam a produção de «artigos» na aceção do artigo 3º, ponto 3, do mesmo regulamento, de substâncias ou misturas	Diretiva 2022/2555, art. 3º., n. 2.
2.4	Empresas do setor alimentar, na aceção do artigo 3º, ponto 2, do Regulamento (CE) nº. 178/2002 do Parlamento Europeu e do Conselho (3), que se dedicam à distribuição por grosso e à produção e transformação industriais, **que não excedam os limiares para as médias empresas previstos no artigo 2º, nº 1, do anexo da Recomendação 2003/361/CE**	Diretiva 2022/2555, art. 3º., n. 2 (variante de limiar inferior a médias empresas, conforme item 1.25 *retro*)
2.5	Entidades que fabricam dispositivos médicos na aceção do artigo 2º, ponto 1, do Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, e entidades que fabricam dispositivos médicos para diagnóstico in vitro na aceção do artigo 2º, ponto 2, do Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho, com exceção das entidades que fabricam dispositivos médicos referidas no anexo I, ponto 5, quinto travessão, da Diretiva 2022/2555	Diretiva 2022/2555, art. 3º., n. 2.
2.6	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 26, da NACE Rev. 2	Diretiva 2022/2555, art. 3º., n. 2.
2.7	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 27, da NACE Rev. 2	Diretiva 2022/2555, art. 3º., n. 2.
2.8	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 28, da NACE Rev. 2	Diretiva 2022/2555, art. 3º., n. 2.
2.9	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 29, da NACE Rev. 2	Diretiva 2022/2555, art. 3º., n. 2.

2.10	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 30, da NACE Rev. 2	Diretiva 2022/2555, art. 3º., n. 2.
2.11	Prestadores de serviço de plataformas de serviços de redes sociais	Diretiva 2022/2555, art. 3º., n. 2.
2.12	Organismos de investigação	Diretiva 2022/2555, art. 3º., n. 2.
2.13	Os operadores de um ponto de carregamento que são responsáveis pela gestão e operação de um ponto de carregamento que presta um serviço de carregamento aos utilizadores finais, incluindo em nome e por conta de um prestador de serviços de mobilidade, **que excedam os limiares para as médias empresas previstos no artigo 2º, nº 1, do anexo da Recomendação 2003/361/CE**.	Diretiva 2022/2555, art. 3º., n. 2 (variante de limiar inferior a médias empresas, conforme item 1.4 *retro*).
2.14	Entidades da administração pública a nível regional tal como definidas por um Estado-Membro em conformidade com o direito nacional	Diretiva 2022/2555, art. 3º., n. 2
2.15	Prestadores de serviços geridos (TIC), **que excedam os limiares para as médias empresas previstos no artigo 2º, nº 1, do anexo da Recomendação 2003/361/CE**	Diretiva 2022/2555, art. 3º., n. 2 (variante de limiar inferior a médias empresas, conforme item 1.22 *retro*).
2.16	Prestadores de serviços de segurança geridos (TIC), **que excedam os limiares para as médias empresas previstos no artigo 2º, nº 1, do anexo da Recomendação 2003/361/CE**	Diretiva 2022/2555, art. 3º., n. 2 (variante de limiar inferior a médias empresas, conforme item 1.23 *retro*).

QUADRO II ENTIDADES DE APLICAÇÃO OBRIGATÓRIA	
1. Regra geral (médias empresas nos termos do artigo 2.º, 1, da Recomendação 2003/361/CE, ou que excedam ditos limiares):	
1.1	Operadores de um ponto de carregamento de energia elétrica que são responsáveis pela gestão e operação de um ponto de carregamento que presta um serviço de carregamento aos utilizadores finais, incluindo em nome e por conta de um prestador de serviços de mobilidade
1.2	Entidades de gestão de serviços TIC (entre empresas) contempladas no item 9 do Anexo I da SRI2
1.3	Prestadores de serviços postais na aceção do artigo 2º, ponto 1-A, da Diretiva 97/67/CE, incluindo prestadores de serviços de estafeta (item 1 do Anexo II da SRI2)
1.4	Empresas que realizam a gestão de resíduos na aceção do artigo 3º, ponto 9, da Diretiva 2008/98/CE do Parlamento Europeu e do Conselho, mas excluindo as empresas para as quais a gestão de resíduos não constitui a atividade económica principal (item 2 do Anexo II da SRI2)

1.5	Empresas que realizam a produção de substâncias e a distribuição de substâncias ou misturas, referidas no artigo 3º, pontos 9 e 14, do Regulamento (CE) nº 1907/2006 do Parlamento Europeu e do Conselho e empresas que realizam a produção de «artigos» na aceção do artigo 3º, ponto 3, do mesmo regulamento, de substâncias ou misturas (item 3 do Anexo II da SRI2)
1.6	Setores e subsetores da indústria transformadora, conforme item 5 do Anexo II da SRI2
1.7	Prestadores de serviços digitais identificados no item 6 do Anexo II da SRI2
1.8	Organismos de investigação, conforme item 7 do Anexo II da SRI2
2) Exceção à regra geral (qualquer dimensão): **2.a) Artigo 2.º, item 2, da SRI2:**	
2.a.1	Fornecedores de redes públicas de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público
2.a.2	Prestadores de serviços de confiança
2.a.3	Registos de nomes de domínio de topo e prestadores de serviços de sistemas de nomes de domínio
2.a.4	Hipótese de entidade que é o único prestador, num Estado-Membro, de um serviço que é essencial para a manutenção de atividades societais ou económicas críticas
2.a.5	Hipótese em que uma perturbação do serviço prestado pela entidade possa afetar consideravelmente a segurança pública, a proteção pública ou a saúde pública
2.a.6	Hipótese em que uma perturbação do serviço prestado pela entidade possa gerar riscos sistémicos consideráveis, especialmente para os setores onde tal perturbação possa ter um impacto transfronteiriço
2.a.7	Hipótese em que a entidade é crítica devido à sua importância específica, a nível nacional ou regional, para o setor ou o tipo de serviço em causa, ou para outros setores interdependentes no Estado-Membro
2.a.8	Entidade da administração pública do governo central, tal como definida por um Estado-Membro em conformidade com o direito nacional
2.a.9	Entidade a nível regional, tal como definida por um Estado-Membro em conformidade com o direito nacional, que, na sequência de uma avaliação baseada no risco, presta serviços cuja perturbação seria suscetível de ter um impacto significativo nas atividades societais ou económicas críticas.

2.b) artigo 2.°, item 3, da SRI2:	
2.b.1	Todas as entidades dos setores e subsetores de energia contemplados no Anexo I da SRI2, exceto os operadores identificados no item 1.1 deste quadro, acima (não incluído no item 1 do Anexo de entidades críticas da Diretiva (EU) 2022/2557)
2.b.2	Todas as entidades dos setores e subsetores de transportes constantes no item 2 do Anexo da Diretiva (EU) 2022/2557 (correspondente ao item 2 do Anexo I da SRI2, com acréscimo do subsetor de transportes públicos)
2.b.3	Todas as entidades do setor bancário indicadas no item 3 do Anexo da Diretiva (EU) 2022/2557 (correspondente ao item 3 do Anexo I da SRI2)
2.b.4	Entidades do setor de infraestruturas do mercado financeiro do item 4 do Anexo da Diretiva (EU) 2022/2557 (correspondente ao item 4 do Anexo I da SRI2)
2.b.5	Todas as entidades dos setores e subsetores de saúde constantes item 5 do Anexo da Diretiva (EU) 2022/2557 (correspondente ao item 2 do Anexo I da SRI2, com acréscimo das entidades titulares de uma autorização de distribuição a que se refere o artigo 79° da Diretiva 2001/83/CE)
2.b.6	Setor de água potável (item 6 do Anexo da Diretiva (EU) 2022/2557, correspondente ao item 6 do Anexo I da SRI2)
2.b.7	Setor de águas residuais (item 7 do Anexo da Diretiva (EU) 2022/2557, correspondente ao item 7 do Anexo I da SRI2)
2.b.8	Todas as entidades dos setores e subsetores de infraestruturas digitais constantes no item 8 do Anexo da Diretiva (EU) 2022/2557 (correspondente ao item 8 do Anexo I da SRI2)
2.b.9	Operadores de infraestruturas terrestres detidas, geridas e operadas pelos Estados-Membros ou por entidades privadas que apoiam a oferta de serviços espaciais, excluindo os fornecedores de redes públicas de comunicações eletrónicas na aceção do artigo 2°, ponto 8, da Diretiva (UE) 2018/1972 (item 10 do Anexo da Diretiva (EU) 2022/2557 (correspondente ao item 11 do Anexo I da SRI2)
2.b.10	Empresas do setor alimentar na aceção do artigo 3°, ponto 2, do Regulamento (CE) n° 178/2002 do Parlamento Europeu e do Conselho, que estejam envolvidas exclusivamente na logística e na distribuição por grosso e produção e transformação industriais em grande escala, conforme item 11 do Anexo da Diretiva (EU) 2022/2557
2.c) artigo 2.°, item 4, da SRI2: entidades prestadoras de serviços de registo de nomes de domínio.	

ANEXO 2: Medidas de supervisão		
Entidades essenciais (artigo 32, n.° 2)	**Entidades importantes (artigo 33, n.° 2)**	**Diferenças**
a) Inspeções no local e supervisão remota, incluindo controlos aleatórios efetuados por profissionais qualificados	a) Inspeções no local e supervisão ex post remota efetuadas por profissionais qualificados	Para entidades essenciais, a supervisão pode ser ex ante, com controles aleatórios; para entidades importantes, a supervisão é ex post
b) Auditorias de segurança regulares e específicas realizadas por um organismo independente ou por uma autoridade competente	b) Auditorias de segurança específicas realizadas por um organismo independente ou por uma autoridade competente	Para entidades essenciais, deve haver auditorias regulares e específicas; para entidades importantes, basta que sejam auditorias específicas
c) Auditorias ad hoc, incluindo em casos justificados por um incidente significativo ou por infração à presente diretiva por parte da entidade essencial	Sem equivalência	Não há previsão de auditorias ad hoc para entidades importantes; apenas para entidades essenciais
d) Verificações de segurança com base em critérios de avaliação dos riscos objetivos, não discriminatórios, equitativos e transparentes, se necessário em cooperação com a entidade em causa	c) Verificações de segurança com base em critérios de avaliação dos riscos objetivos, não discriminatórios, equitativos e transparentes, se necessário em cooperação com a entidade em causa	Previsões idênticas
e) Pedidos de informações necessárias para avaliar as medidas de gestão dos riscos de cibersegurança adotadas pela entidade em causa, incluindo políticas de cibersegurança documentadas, bem como o cumprimento da obrigação de apresentar informações às autoridades competentes nos termos do artigo 27	d) Pedidos de informações necessárias para avaliar ex post as medidas de gestão dos riscos de cibersegurança adotadas pela entidade em causa, incluindo políticas de cibersegurança documentadas, bem como o cumprimento da obrigação de apresentar informações às autoridades competentes nos termos do artigo 27	A distinção está em que a avaliação das medidas de gestão dos riscos de cibersegurança é ex post para entidades importantes; não há esta restrição aos órgãos fiscalizatórios em relação às entidades essenciais
f) Pedidos de acesso a dados, documentos e informações necessárias para o desempenho das funções de supervisão	e) Pedidos de acesso a dados, documentos e quaisquer informações necessárias para o desempenho das suas funções de supervisão	Previsões idênticas
g) Pedidos de provas da aplicação das políticas de cibersegurança, como os resultados de auditorias de segurança efetuadas por um auditor qualificado e os respetivos elementos de prova subjacentes	f) Pedidos de provas da aplicação das políticas de cibersegurança, como os resultados de auditorias de segurança efetuadas por um auditor qualificado e os respetivos elementos de prova subjacentes	Previsões idênticas

ANEXO 3		
Medidas de execução		
Entidades essenciais (artigo 32, n.º 4)	**Entidades importantes (artigo 33, n.º 4)**	**Diferenças**
a) Emitir advertências sobre infrações à presente diretiva por parte das entidades em causa	a) Emitir advertências sobre infrações à presente diretiva por parte das entidades em causa	Previsões idênticas
b) Adotar instruções vinculativas, inclusivamente em relação às medidas necessárias para impedir ou corrigir um incidente, bem como aos prazos para executar essas medidas e para informar sobre a sua execução, ou uma ordem que exija que as entidades em causa corrijam as deficiências detetadas ou as infrações à presente diretiva	b) Adotar instruções vinculativas ou uma ordem que exija que as entidades em causa corrijam as deficiências detetadas ou as infrações à presente diretiva	Para entidades essenciais, o dispositivo assevera expressamente que as instruções vinculativas incluem as "medidas necessárias para impedir ou corrigir um incidente, bem como aos prazos para executar essas medidas e para informar sobre a sua execução"
c) Ordenar que as entidades em causa cessem condutas que infrinjam a presente diretiva e se abstenham de as repetir	c) Ordenar que essas entidades cessem condutas que infrinjam apresente diretiva e se abstenham de as repetir	Previsões idênticas
d) Ordenar que as entidades em causa garantam que as suas medidas de gestão dos riscos de cibersegurança cumpram o disposto no artigo 21 ou cumpram as obrigações de notificação estabelecidas no artigo 23 de uma forma e num período especificados	d) Ordenar que as entidades em causa garantam que as suas medidas de gestão dos riscos de cibersegurança cumpram o disposto no artigo 21 ou cumpram as obrigações de notificação estabelecidas no artigo 23 de uma forma e num período especificados	Previsões idênticas
e) Ordenar que as entidades em causa informem as pessoas singulares ou coletivas a quem prestam serviços ou levam a cabo atividades que sejam potencialmente afetadas por uma ciberameaça significativa da natureza da ameaça, bem como de quaisquer possíveis medidas de proteção ou corretivas que possam ser tomadas por essas pessoas em resposta a essa ameaça	e) Ordenar que as entidades em causa informem as pessoas singulares ou coletivas a quem prestam serviços ou levam a cabo atividades que sejam potencialmente afetadas por uma ciberameaça significativa da natureza da ameaça, bem como de quaisquer possíveis medidas de proteção ou corretivas que possam ser tomadas por essas pessoas singulares ou coletivas em resposta a essa ameaça	Previsões idênticas
f) Ordenar que as entidades em causa apliquem, num prazo razoável, as recomendações formuladas em resultado de uma auditoria de segurança	f) Ordenar que as entidades em causa apliquem, num prazo razoável, as recomendações formuladas em resultado de uma auditoria de segurança	Previsões idênticas

g) Designar um supervisor com funções bem definidas durante um determinado período para supervisionar o cumprimento pelas entidades em causa dos artigos 21 e 23	Sem equivalência	A designação de um supervisor temporário é apenas para entidades essenciais
h) Ordenar que as entidades em causa tornem públicos os aspetos das infrações à presente diretiva de uma determinada forma	g) Ordenar que essas entidades tornem públicos os aspetos das infrações à presente diretiva de uma determinada forma	Previsões idênticas
i) Impor ou solicitar a imposição, por parte dos organismos ou tribunais competentes, em conformidade com o direito nacional, de uma coima nos termos do artigo 34, em complemento de qualquer uma das medidas referidas nas alíneas a) a h) do presente número	h) Impor ou solicitar a imposição, por parte dos organismos ou tribunais competentes, em conformidade com o direito nacional, de uma coima nos termos do artigo 34, em complemento de qualquer uma das medidas referidas nas alíneas a) a g) do presente número	Previsões idênticas

ANEXO 4	
Medidas de execução (entidades essenciais)	
Entidades essenciais (artigo 32, n.° 5)	**Entidades importantes**
Sempre que as medidas de execução adotadas nos termos do n° 4, alíneas a) a d) e f), se revelarem ineficazes, os Estados-Membros devem assegurar que as suas autoridades competentes dispõem de poderes para estabelecer um prazo dentro do qual se solicita à entidade essencial que tome as medidas necessárias para corrigir as deficiências ou cumprir os requisitos dessas autoridades. **Se a medida solicitada não for tomada dentro do prazo estabelecido, os Estados-Membros devem assegurar que as suas autoridades competentes dispõem de poderes para:**	Sem equivalência
a) Suspender temporariamente ou solicitar a um organismo de certificação ou autorização, ou a um tribunal, em conformidade com o direito nacional, a suspensão temporária de uma certificação ou autorização relativa a uma parte ou à totalidade dos serviços relevantes prestados ou das atividades levadas a cabo pela entidade essencial	Sem equivalência
b) Solicitar que os organismos ou tribunais competentes, em conformidade com o direito nacional, proíbam temporariamente qualquer pessoa singular com responsabilidades de gestão a nível de diretor executivo ou de representante legal de exercer funções de gestão nessa entidade essencial	Sem equivalência

ANEXO 5	
Parâmetros para aplicação de sanções	
Diretiva (UE) 2022/2555 (artigo 34.°, n.° 3 c/c artigo 32.°, n.° 7)	**Decreto-Lei n.° 433/1982 (artigo 18.°) Repleto de conceitos indeterminados**
a) A gravidade da infração e a importância das disposições violadas, sendo que, em qualquer circunstância, devem ser consideradas infrações graves as seguintes infrações: i) violações repetidas, ii) não notificação ou não correção de incidentes significativos, iii) não correção de deficiências na sequência de instruções vinculativas das autoridades competentes, iv) obstrução de auditorias ou atividades de acompanhamento ordenadas pela autoridade competente na sequência da constatação de uma infração, v) prestação de informações falsas ou grosseiramente inexatas em relação às medidas de gestão dos riscos de cibersegurança ou às obrigações de notificação estabelecidas nos artigos 21.° e 23.°	Gravidade da contraordenação
b) A duração da infração	
c) Quaisquer anteriores infrações relevantes cometidas pela entidade em causa	
d) Quaisquer danos materiais ou imateriais causado, incluindo quaisquer prejuízos financeiros ou económicos, os efeitos noutros serviços e o número de utilizadores afetados	
e) Qualquer intenção ou negligência do autor da infração	Culpa
f) Quaisquer medidas tomadas pela entidade para prevenir ou atenuar os danos materiais ou imateriais	
g) Qualquer cumprimento de códigos de conduta ou procedimentos de certificação aprovados	
h) O nível de cooperação das pessoas singulares ou coletivas consideradas responsáveis com as autoridades competentes	
	Situação económica do agente
	Benefício económico que este retirou da prática da contraordenação

Sobre os Autores

Graça Enes

Licenciada e Mestre em Direito pela Faculdade de Direito da Universidade de Coimbra. Doutorada em Direito pela Faculdade de Direito da Universidade do Porto.
Diretora do CIJ (2021-).
Titular do Módulo Jean Monnet DigEUCit "A Digital Europe for Citizens. Constitutional and Policymaking Challenges".
Além do Direito da União Europeia, os seus interesses científicos e académicos estendem-se ao Direito Internacional e aos novos desafios da governance política internacional, em especial o espaço digital e o ambiente.
Foi Subdiretora da FDUP (2013-2014) e Diretora do 2º Ciclo de Estudos em Direito (2019-2020). É membro da Associação Portuguesa de Direito Europeu e da Associação de Direito e Economia Europeia.
Investigadora Associada do Institut de Recherche en Droit européen et international comparé, da Université Toulouse Capitole.
Co-Coordenadora do Núcleo Português do European Law Institute

Augusto Batalha Monteiro

Augusto Batalha Monteiro é brasileiro, nasceu na cidade de São Luís, no Estado do Maranhão, em 1983.
Licenciou-se em Direito na Universidade Federal do Maranhão em 2008.
Iniciou suas atividades profissionais como assessor de Juiz de Direito, ainda em 2008; posteriormente, exerceu atividades de assessoramento a membros do Ministério Público Federal, de 2009 a 2015, e da Magistratura Federal, de 2015 a 2017.
Desde 2017, é membro da Advocacia-Geral da União, na qual exerce o cargo de Advogado da União, na Procuradoria da União no Estado do Maranhão.
É mestrando em Ciências Jurídico-Políticas na Faculdade de Direito da Universidade do Porto.

Flávia Oliveira

Licenciada em Direito (1996) pela Faculdade de Direito da Universidade Católica de Santos, SP, Brasil, com pós-graduação lato sensu (1996/1997), na mesma instituição, em Direito Processual Civil.
Procuradora do Município de Santos desde 30 de outubro de 2006, onde exerceu os cargos de Assistente da Procuradora-Geral do Município e Chefe da Procuradoria Fiscal do Município, atualmente em regime de licença.
Aluna do curso de Mestrado em Ciências Jurídico-Políticas da Faculdade de Direito da Universidade do Porto, em fase de conclusão.

Sobre os CIJ-RP (CIJ Research Papers / Cadernos de Investigação do CIJ)

Os CIJ-RP são uma série de publicações disponibilizadas em linha que dão a conhecer à comunidade a reflexão desenvolvida no âmbito de projetos de investigação, em comunicações e outras atividades científicas, académicas e de formação, da autoria de investigadores do CIJ, de investigadores visitantes e convidados, bem como estudantes de doutoramento e de mestrado da FDUP. Os CIJ-RP são o testemunho do compromisso com o objetivo da ciência aberta, ao serviço da sociedade. As línguas de publicação são o português e o inglês, podendo excecionalmente a publicação ocorrer em outra língua.

Sobre o CIJ

O Centro de Investigação Interdisciplinar em Justiça (CIJ) é uma Unidade de Investigação e Desenvolvimento integrada na Faculdade de Direito da Universidade do Porto (FDUP). Ramifica a sua investigação em quatro eixos: (1) Direito, Sociedade e Poder, (2) Negócios, Empresas e Mercados (3) Dinâmicas Transnacionais, Transição Verde e Digital e (4) Crime, Segurança e Vitimação.

CIJ
CENTRO DE INVESTIGAÇÃO
INTERDISCIPLINAR
EM JUSTIÇA