REVISTA ELECTRÓNICA DE DIREITO

RED

Os serviços de iniciação de pagamento no novo RSP

Payment initiation services in the new Portuguese payment services act

Patrícia Alexandra Paiva Duarte

Mestre em Direito pela FDUP

Advogada-estagiária na AdC Advogados

Rua Oliveira Martins, n.º 63, 4200-429 Porto, Portugal

patriciapaivaduarte@gmail.com

https://orcid.org/0000-0003-0007-8804

Junho de 2021

RESUMO: Os serviços de pagamento tradicionais têm sido substituídos pela utilização de dispositivos móveis e por novas soluções desenvolvidas por *FinTechs* que vêm difundir a ideia de um pagamento mais seguro e rápido junto dos consumidores. Na sequência destas inovações, o novo Regime Jurídico dos Serviços de Pagamento veio estender o seu âmbito de aplicação ao incluir novas atividades no que respeita aos serviços de pagamento, nomeadamente os serviços de iniciação de pagamentos, sobre os quais iremos verter a nossa atenção. Assim, propomo-nos a indagar sobre a proteção do utilizador – e consumidor – perante a prestação desses serviços por terceiras entidades, em duas dimensões essenciais da sua proteção: a tutela dos seus dados pessoais e a proteção perante a fraude nos pagamentos eletrónicos. Desta forma, importa perspetivar a relação estabelecida entre os novos prestadores de serviços de iniciação não só com o utilizador, mas também com o prestador que permite o acesso à conta que gere, em relação à qual a lei nem sempre surge esclarecedora, designadamente em matéria de autenticação e repartição objetiva do risco de operações de pagamento não autorizadas.

PALAVRAS-CHAVE: serviços de iniciação de pagamentos; terceiros prestadores; *open banking*; proteção de dados; consentimento; operações de pagamento não autorizadas; autenticação forte.

ABSTRACT: Traditional payment services have been replaced by the use of mobile devices and by new solutions developed by FinTechs that spread the idea of safer and faster payments among consumers. Along with these innovations, the new Portuguese payment services act has extended its scope to include new activities regarding payment services, namely payment initiation services, on which we will focus our attention. Thus, we propose to inquire about user protection, regarding the provision of those services by third parties, in two essential dimensions of his protection, the safeguarding of his personal data and the protection against fraud on electronic payments. In light of this, it is important to envision the relationship established between this new initiation services providers, not only with the user, but also with the provider, who provides and maintains the account, to which the law doesn't always appear enlightening, namely in terms of authentication and objective sharing of the risks of unauthorized payment transactions.

KEY WORDS: payment initiation services; third party providers; open banking; data protection; consent; unauthorized payment transactions; strong authentication.

SUMÁRIO:

1. Introdução: da DSP à DSP2

A última década, marcada por uma crescente inovação tecnológica, introduziu significativas alterações nos modos de consumo de particulares e empresas, nomeadamente, através do protagonismo do comércio em linha, do reconhecimento de intermediadores eletrónicos e pelo surgimento da prestação de novos serviços financeiros, essencialmente associados ao comércio eletrónico.

De modo a acompanhar o dinamismo tecnológico e manter a eficiência e integração do mercado interno, a Comissão Europeia iniciou, em 2012, com o Livro Verde para um mercado europeu integrado dos pagamentos[1], o processo que antecedeu uma nova iniciativa legislativa. Publicada em 25 de novembro de 2015, a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho (DSP2), em matéria de Serviços de Pagamento no mercado interno, veio substituir a primeira Diretiva do Serviços de Pagamento (DSP)[2], que havia surgido como fruto do objetivo de concretizar um mercado integrado de pagamentos, almejando uniformizar as soluções praticadas em matéria de serviços de pagamento entre os vários Estados-Membros.

A nova Diretiva optou pela revogação da anterior, mas não configura uma alteração substancial do quadro jurídico estabelecido pela DSP, mantendo, na essencialidade, a mesma sistematização, terminologia e soluções. Não deixa, porém, de introduzir novidades significativas que vêm trazer, ao abrigo do objetivo de o tornar cada vez mais digital, um novo paradigma para o mercado dos serviços de pagamento, requerendo um esforço de adaptação devido à exigência de um maior desenvolvimento técnico dos instrumentos de pagamento disponibilizados e das infraestruturas dos prestadores de serviço[3].

O conjunto de derrogações previsto na DSP contribuiu para um quadro regulamentar relativamente distinto entre os Estados, mantendo um mercado de pagamentos fragmentado, com soluções e custos díspares, identificado pela Comissão Europeia[4] como uma das principais barreiras ao crescimento do comércio eletrónico[5] e permitiu, paralelamente, o desenvolvimento de novos serviços que instalaram um ambiente de insegurança jurídica e

[1] COMISSÃO EUROPEIA, *Livro Verde – Para um mercado europeu integrado dos pagamentos por cartão, por Internet e por telemóvel*, COM(2011) 941 final, Bruxelas, 2012, disponível em https://www.ec.europa.eu (04.03.2020).
[2] Diretiva 2007/64/CE do Parlamento Europeu e do Conselho, de 13 de novembro de 2007, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE e revoga a Diretiva 97/5/CE, *in JO L 319 de 5.12.2007.* A DSP foi transposta para a ordem portuguesa a 30 de outubro de 2009 no Anexo I ao Decreto-Lei n.º 317/2009, surgindo, deste modo, o primeiro Regime Jurídico dos Serviços de Pagamento. Foi, entretanto, revogada pela Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE, *in JO L 337 de 23.12.2015*.
[3] *Vide* FRANCISCO MENDES CORREIA, "Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento" *in III Congresso de Direito Bancário,* VASCONCELOS, L. Miguel Pestana de (Coord.), Coimbra, Edições Almedina, 2018, p. 386.
[4] COMISSÃO EUROPEIA, *Livro Verde*..., cit., p. 5.
[5] JAVIER SANTAMARIA, "La segunda Directiva de Servicios de Pago y sus impactos en el mercado", *in Observatorio de Divulgación Financiera,* Nota Técnica n.º 31*,* Instituto de Estudios Financieros, 2018, disponível em https://www.iefweb.org (27.09.2019), pp. 2-3. Ainda sobre as dificuldades da DSP, ver ALAN BRENER, "Payment Service Directive II and Its Implications", *in Disrupting Finance. FinTech and Strategy in the 21st Century,* Palgrave Pivot, Cham*,* 2019, disponível em https://link.springer.com, pp. 105-108.

enfraqueceram a proteção do consumidor[6], uma vez que a prestação desses serviços não se encontrava vinculada às obrigações previstas na DSP, nem estava configurada a amplitude da responsabilidade de quem os presta[7]. Esta circunstância permitiu que entidades pudessem oferecer os mesmos serviços que os prestadores obrigados pela Diretiva, com custos inferiores e com maior liberdade no modo de os prestar, o que lhes permitiu aprimorar e inovar a sua prestação.

Por sua vez, assistiu-se a um aumento da utilização de dispositivos móveis mediante aplicações bancárias e de pagamento, transferindo o *homebanking,* acedido através de um computador, para aplicações instaladas em telemóveis[8]. Esta evolução surgiu paralelamente aos mais variados e sofisticados tipos de fraude e, com isso, a necessidade de melhor se proteger os interesses dos utilizadores e a segurança na execução dos pagamentos.

Em seguimento surge a DSP2, por um lado, como resposta à inovação e com intuito de promover uma livre e leal concorrência em matéria de serviços de pagamento, concedendo abertura a novas entidades[9] num mercado tradicionalmente fechado, configurando-se tal abertura como necessária para melhorar a prestação oferecida ao consumidor e, consequentemente, a sua confiança no sistema de pagamentos europeu. Por outro, vem com a preocupação primordial de reforçar a segurança e a proteção do consumidor, visando dar resposta às adicionais exigências e desafios do ponto de vista regulamentar.

É em decorrência da transposição desta iniciativa legislativa europeia que surge o nosso novo Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RSP), aprovado em anexo ao Decreto-Lei n.º 91/2018, de 12 de novembro[10] e que transpôs em moldes quase idênticos o texto da Diretiva[11].

1.1. O *Open Banking* e os novos atores: em especial, o Prestador de Serviços de Iniciação de Pagamentos (PSIP)

[6] PEGGY VALCKE; NIELS VANDEZANDE; NATHAN VAN DE VELDE, *The Evolution of Third Party Payment Providers and Cryptocurrencies Under the EU's Upcoming PSD2 and AMLD4*, SWIFT Institute Working Paper n.º 2015-001, 2015, disponível em https://swiftinstitute.org (27.03.2021), p. 12.
[7] Considerandos 4 e 7 da DSP2.
[8] *Vide* MARIA RAQUEL GUIMARÃES, "Pagamentos electrónicos não autorizados e fraudulentos", [*in Cibercriminalidade: novos desafios, ofensas e soluções* (em revisão), I. Guedes & M. Gomes (Eds.), Lisboa, PACTOR – Edições de Ciências Sociais, Forenses e da Educação] (em curso de publicação), n.º 1. A Autora fala em "mobilização" da banca eletrónica, alertando para os novos perigos destes dispositivos móveis.
[9] Neste âmbito, têm ganho algum destaque as entidades de tecnologia financeira, vulgarmente denominadas por *FinTech*, por aproveitarem o uso da tecnologia na atividade financeira em contraposição às instituições tradicionais, têm sido, como expõe o administrador do Banco de Portugal, HÉLDER ROSALINO, "responsáveis pelo desenvolvimento de novas plataformas tecnológicas que permitem a distribuição de produtos e a prestação de serviços financeiros de uma forma mais célere, conveniente, adaptada às necessidades dos clientes, intuitiva e, por vezes, com custos mais baixos". *Vide* HÉLDER ROSALINO, "FinTech e banca digital", *in FinTech: Desafios da Tecnologia Financeira,* CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Coord.), Coimbra, Edições Almedina, 2017, p. 10.
[10] A transposição da DSP2 para a nossa ordem jurídica deu-se já depois do prazo limite para a sua transposição, o que impunha que a mesma fosse realizada até 13 de janeiro de 2018.
[11] As disposições mencionadas no presente estudo que não sejam precedidas de referência ao diploma a que pertencem, referem-se ao regime anexo ao Decreto-Lei n.º 91/2018, de 12 de novembro.

A adesão do consumidor a novas soluções implicou alterações ao quadro tradicional que marcava o mercado dos serviços de pagamento e obrigou o reconhecimento de novos serviços e da possibilidade de tais serviços serem prestados por operadores que não gerem uma conta de pagamento, pelo que a DSP2 optou por consagrar o *Open Banking* (operação bancária aberta) que se configura num "modelo colaborativo nos termos do qual são partilhados dados bancários"[12] e que obriga as instituições de crédito a permitir o acesso às informações por elas detidas. A par disso, cabe aos bancos adotar todas as medidas necessárias para permitir que as novas entidades consigam obter esse acesso e usar a informação detida pelos mesmos, que é essencial ao desenvolvimento das suas atividades[13].

Embora o reconhecimento desta abertura configure um desafio aos operadores tradicionais que detinham o protagonismo no mercado dos serviços de pagamento, surge também como a melhor forma de acautelar a posição dos utilizadores, uma vez que vem estabelecer os requisitos necessários para um acesso e comunicação de dados seguros, permitindo-se que os terceiros prestadores não tenham um automático acesso a todas as informações que constam na conta de pagamento.

Posto isto, as atividades que consubstanciam serviços de pagamentos nos termos do novo RSP não sofreram grandes alterações[14], com a exceção de acolher juridicamente duas espécies de novos serviços de pagamento especializados "em fases ou dimensões especificas dos serviços de pagamento"[15], que deriva do surgimento, já na vigência do anterior regime, de serviços especializados na iniciação de operações de pagamento e de serviços complementares que recolhem, agregam e disponibilizem informação sobre as contas de pagamento dos utilizadores. São atividades que podem ser desempenhadas por operadores externos à relação existente entre o utilizador e o prestador de serviço de pagamentos que lhe fornece e gere uma conta de pagamento, na maioria dos casos, as instituições bancárias. São por isso denominados por terceiros prestadores de serviços (*Third Party Providers*), reconfigurando a relação que os utilizadores estabelecem com o seu banco e o modo de execução das transações[16].

Definidos nas al. nn) e tt), do art. 2.º, o prestador de serviços de informação sobre contas (PSIC)[17] tem como atividade fornecer ao utilizador de serviços de pagamento informações agregadas em linha sobre as contas que este possa deter junto de outro prestador de serviços,

---

[12] *Vide* TIAGO CORREIA MOREIRA; INÊS ANTAS DE BARROS; ISABELA ORNELAS, "Partilha de dados pessoais e operação bancária aberta", *in Fintech II: Novos Estudos sobre Tecnologia Financeira,* CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Coord.), Coimbra, Edições Almedina, 2019, p. 148.

[13] A ideia de *Open Banking* desenvolveu-se também no Reino Unido através do projeto *Open Banking Standard*, o que obrigou as entidades aderentes a "estandardizar os dados relativos às contas correntes e produtos bancários de retalho" para permitir o acesso a terceiros, *vide* TIAGO CORREIA MOREIRA; INÊS ANTAS DE BARROS; ISABELA ORNELAS, "Partilha de dados pessoais...", cit., p. 149, nota de rodapé 1.

[14] *Vide* RITA MAFALDA VERA-CRUZ PINTO BAIRROS, "A transferência a crédito – Notas caracterizadoras no contexto SEPA e do Regime Jurídico dos Serviços de Pagamento", *in Cadernos O Direito – Temas de Direito Bancário I,* n.º 8, Coimbra, Edições Almedina, , 2014, p. 253.

[15] *Vide* FRANCISCO MENDES CORREIA, "Uma revolução permanente? A DSP 2...", cit., p. 395.

[16] O considerando 21 da DSP2 salienta que a definição de serviços de pagamento é tecnologicamente neutra de forma a englobar o surgimento de novos serviços.

[17] Na versão inglesa da DSP2, lê-se "*Account Information Service Provider – AISP*".

agora definidos, na al. qq) do citado artigo, como o "prestador de serviços de pagamento que gere a conta" (PSPGC)[18]. O objetivo é oferecer ao utilizador uma visão global da sua situação financeira ao consultar o instrumento (v.g. aplicação de telemóvel)[19] que o PSIC lhe disponibiliza[20].

A par disso, e sobre os quais melhor incidem o nosso estudo, a alínea g) do art. 4.º, vem ditar a aplicação do novo regime jurídico ao prestador de serviços de iniciação de pagamentos (PSIP)[21]. Este tipo de serviço surgiu em decorrência do desenvolvimento do comércio eletrónico que exigiu alternativas seguras para a realização dos pagamentos, de modo a superar o receio e insegurança sentidos pelo consumidor ao fornecer diretamente os dados do seu cartão de débito ou crédito na página do comerciante[22]. A utilização de cartões como meio primordial de pagamento na Internet colocava entraves "a potenciais clientes que não disponham deste tipo de pagamento"[23].

O novo RSP transpõe na íntegra a definição dada pela DSP2, estabelecendo na al. uu), do art. 2.º, que o serviço de iniciação de pagamentos é "um serviço de pagamento que consiste em iniciar uma ordem de pagamento a pedido do utilizador de serviços de pagamento relativamente a uma conta de pagamento por si titulada noutro prestador de serviços de pagamento". Para melhor entender o enquadramento e funcionamento destes serviços, o considerando 27 da DSP2 refere que tais serviços de pagamento criam uma "ponte telemática"

[18] Em inglês, "*Account Servicing Payment Service Provider – ASPSP*".
[19] O Money Dashboard é um exemplo de um prestador de serviços de informação sobre contas britânico, surgido ainda na vigência da DSP, que permite aos utilizadores conectar as várias contas *online* que possuem em diferentes bancos e cartões de crédito, *vide* https://www.moneydashboard.com/our-story (09.02.2020). Em Portugal, como exemplo da prestação deste tipo de serviços temos a recente aplicação DABOX da Caixa Geral de Depósitos, que pretende agregar as informações sobre "os saldos e movimentos das contas à ordem" que o utilizador possui em várias instituições, permitindo ao utilizador categorizar os gastos e definir orçamentos tendo por base todas as contas de pagamento e fundos que possui, de modo a facultar orientações personalizadas para ajudar na gestão financeira pessoal. Cfr. https://www.dabox.pt (09.02.2020).
[20] *Vide* considerando 28 da DSP2.
[21] Em inglês, "*Payment Initiation Service Provider – PISP*". Cfr. al. oo) e uu), do art. 2.º.
[22] Um dos exemplos mais paradigmáticos que permite ao utilizador a não divulgação direta dos dados de um cartão na página do comerciante, é o caso do Paypal. A realização de pagamentos *online* com o Paypal ganhou, ao longo dos anos, uma grande adesão pelo facto do prestador garantir ao consumidor que os seus dados bancários não eram divulgados perante o beneficiário. O Paypal exerce um serviço semelhante à iniciação de pagamentos, mas não reduz a sua atividade à prestação desses serviços, encontrando-se registado no Banco de Portugal como uma instituição de crédito e definindo-se como instituição de emissão de dinheiro eletrónico. Isto porque, o dinheiro que é enviado entre contas Paypal não se confunde com o dinheiro de circulação comum e é considerado pelo mesmo como dinheiro eletrónico, exigindo-se que o utilizador selecione uma hipótese de financiamento – cartão de crédito ou conta bancária -, de modo a adquirir o dinheiro eletrónico utilizado pelo Paypal, que possui valor idêntico ao dinheiro em numerário. Embora de um ponto de vista prático, a transferência que aqui se aplica assemelha-se à utilização conjunta do *homebanking* e de serviços de iniciação, descortina-se algumas diferenças, veja-se o exemplo do envio de dinheiro de uma conta Paypal a título de doação para outra. O dinheiro eletrónico recebido encontra-se exclusivamente na conta Paypal, podendo o utilizador manter a quantia nessa conta para proceder a futuros pagamentos ou transferi-la para a sua conta bancária. Tal circunstância altera o enquadramento da figura à luz da lei. No contrato de utilização dos serviços Paypal, prevê-se a possibilidade de recorrer a serviços de iniciação em relação a uma conta Paypal. Disponível em https://www.paypal.com/pt/webapps/mpp/ua/useragreement-full (4.11.2019). ANDREW MURRAY expõe precisamente como o Paypal surgiu com o objetivo de se vingar como uma instituição de moeda eletrónica, mas que optou por se registar com a mesma autorização que as instituições de crédito pelo facto dos requisitos aplicáveis às instituições de moeda eletrónica, à luz do anterior regime, serem demasiado restritivos. *Vide* ANDREW MURRAY, *Information Technology Law: The Law & Society*, 4.ª Ed., Oxford, Oxford University Press, 2019, pp. 441-442.
[23] FRANCISCO MENDES CORREIA, "Uma revolução permanente? A DSP 2...", cit., p. 396. O Autor aponta como principais barreiras à dinamização dos pagamentos no seio do comércio eletrónico a falta de celeridade que a inserção dos dados do cartão acarreta, o receio de fraude e apropriação indevida desses dados e os custos associados à utilização de cartões de crédito em pagamentos *online*.

entre a página *online* do comerciante[24] e a plataforma bancária em linha do PSPGC. Ou seja, é necessário que exista uma conta de pagamento *online*, cujo acesso foi disponibilizado ao utilizador. No mesmo sentido dispõe o art. 106.º, n.º 1, do RSP, ao referir que, "se a conta de pagamento for acessível em linha" o utilizador tem o direito de recorrer a tais serviços, ainda que prestados por um terceiro prestador. Há, portanto, uma inerente ligação destes serviços com o *homebanking* disponibilizado pelos bancos. O PSIP atuará como um verdadeiro intermediário entre a página do comerciante e a plataforma *online* do banco do utilizador, mas irá igualmente substituir-se a este último na emissão da ordem de pagamento perante o banco.

1.2. O processo de iniciação do pagamento

A iniciação de pagamentos, conquanto transmita ao consumidor uma maior segurança nos pagamentos no seio do comércio eletrónico, não beneficia única e exclusivamente o utilizador que cede o acesso à sua conta. Uma das principais vantagens associadas é, precisamente, a intermediação existente entre o beneficiário e o PSIP, que lhe confirma, diretamente e com brevidade, a existência de fundos[25] na conta do ordenante e de que foi iniciada a execução do pagamento com vista ao cumprimento da prestação que o contrato celebrado entre o beneficiário e o utilizador originou para este, encorajando o primeiro a enviar ou prestar o seu serviço imediatamente[26]. Vem, deste modo, agilizar o processo inerente ao comércio eletrónico, que pressupunha alguma delonga entre o momento da confirmação da encomenda e a expedição da mesma, devido à comprovação do pagamento por parte do comerciante. Deixa de ser necessário a efetiva receção da quantia, bastando-se com a confirmação, por uma terceira parte qualificada, de que a ordem de pagamento foi emitida e que, assegurada a existência de fundos suficientes, irá receber a quantia acordada[27].

O processo inicia-se quando o consumidor pretende adquirir um bem ou serviço em linha e opte por utilizar um serviço de iniciação[28] no momento da seleção do meio de pagamento, cujo prestador terá de aceder a uma conta de pagamento detida pelo primeiro. Deste modo, o utilizador autoriza o PSIP a emitir uma ordem de pagamento, apondo as credenciais de segurança personalizadas[29] de acesso à sua conta *online* facultadas pelo PSPGC na *interface*

[24] Embora os considerandos da DSP2 façam referência à página do comerciante, o beneficiário poderá ser outro consumidor, o que é frequente em plataformas que permitem agregar uma vasta oferta de produtos por profissionais e consumidores. A referir esta particularidade, *vide* MARIA RAQUEL GUIMARÃES, em "O comércio electrónico ‹‹está na moda››? Algumas questões jurídicas a propósito da oferta de moda ‹‹online››", *in Fashion Law: Direito da Moda,* CASTRO, João Fraga de (Coord.), Cizur Menor, Thomson Reuters Aranzadi, 2019, p. 847.
[25] A pedido do terceiro prestador, sobre o PSPGC recai o dever de confirmar a disponibilidade de fundos suficientes para a execução do pagamento sob a forma de um "sim" ou "não", nos termos do disposto na al. c), do n.º 2, do art. 36º, do Regulamento Delegado (UE) 2018/389 da Comissão de 27 de novembro.
[26] O considerando 29 da DSP2 refere o objetivo de se potencializar a celeridade da disponibilização e envio de encomendas no seio do comércio eletrónico.
[27] PEGGY VALCKE; NIELS VANDEZANDE; NATHAN VAN DE VELDE, *The Evolution of Third Party*…, cit., p. 16.
[28] O Sofort e o iDeal (v. notas 31 e 32) são serviços existentes que possuem modelos de negócio que vão de encontro com o que consiste a iniciação de pagamentos. *Vide* PEGGY VALCKE; NIELS VANDEZANDE; NATHAN VAN DE VELDE, *The Evolution of Third Party*…, cit., p. 16.
[29] As credenciais de segurança personalizadas do utilizador são definidas, no art. 2.º, al. j), como "elementos personalizados fornecidos pelo prestador de serviços de pagamento a um utilizador de serviços de pagamento para efeitos de autenticação". As mesmas visam garantir um acesso e emissão de ordens de pagamento mais

de programação de aplicações[30] (API, de *Application Programming Interface)* que o PSIP lhe apresenta[31] aquando da solicitação do seu serviço ou diretamente na sua página de *homebanking* que lhe surge mediante redireccionamento[32]. Por sua vez, entre o PSIP e o beneficiário, deverá existir um acordo prévio que lhe permita facultar ao PSIP as informações necessárias para que o último possa gerar referências de pagamento automatizadas[33]. Requerido o serviço por parte do adquirente, o PSIP acede à conta e confirma a disponibilidade de fundos para a execução da transferência[34]. Dá-se aí a iniciação da operação de pagamento por parte do PSIP, que comunica ao banco do adquirente os dados do beneficiário para que, competente para se substituir ao utilizador no cumprimento da obrigação perante o seu credor, execute a transferência ordenada através do serviço de iniciação de modo a creditar a conta do beneficiário. Depois da confirmação por parte do PSPGC da iniciação da execução, a mesma é informada ao beneficiário[35].

Como se pode constatar, os prestadores de serviços de iniciação, quando assumem as vestes de terceiro prestador, passam a poder aceder a contas de pagamento dos seus clientes que estão sediadas noutro PSP, desenvolvendo as suas atividades sem que para isso detenham fundos dos mesmos[36]. Certo é que tal acesso já existia anteriormente, mas escapava a

seguros, por permitirem ao PSP verificar a legitimidade do titular do instrumento. A possibilidade de o acesso pelo PSIP dar-se mediante um processo que implique o conhecimento das credenciais fornecidas pelo PSPGC é reconhecido pelo próprio regime, designadamente, no art. 106.º, n.º 3, al. b), que estabelece o dever do PSIP assegurar que as credenciais de segurança personalizadas não sejam acessíveis por terceiros. A mesma possibilidade é reconhecida no considerando 30 da DSP2.

[30] Para maior desenvolvimento sobre as *interfaces*, *vide* JON STIAN GULBRANDSEN EIDE e STIAN HALLUM, "PSD2: A Strategic Perspective on Third-Party Payment Service Providers", dissertação de mestrado, Oslo, BI Norwegian Business School, 2018 (inédita) pp. 58-59. Como referem os Autores, uma *interface* de programação de aplicações permite conectar vários prestadores e a partilha de dados e comunicações entre os mesmos.

[31] O modelo de negócio do Sofort, um prestador de iniciação de pagamentos alemão que foi posteriormente adquirido pela empresa sueca, Klarna, pressupõe que o prestador recolha e utilize as credenciais de segurança do utilizador. O consumidor ao selecionar o Sofort/Klarna na página do comerciante, terá de autenticar-se na API *do mesmo, que irá, após a receção das credenciais, aceder à conta online pelo utilizador e iniciar o pagamento. Este processo é complementado, por razões de segurança, com a introdução de um código de confirmação recebido pelo utilizador. Cfr.* https://www.klarna.com/sofort (7.12.2019).

[32] Como exemplo de uma prática de redireccionamento da autenticação, veja-se o que acontece com o iDeal. O utilizador ao escolher o iDeal como meio de pagamento é redirecionado para a sua página de *homebanking,* onde tem de se autenticar normalmente. Ao entrar na sua conta *online*, os dados para o pagamento já estarão preenchidos, restando apenas a confirmação do pagamento por parte do utilizador. Para mais informações sobre este serviço, *vide* https://www.ideal.nl/en/consumers/what-is-ideal (7.12.2019). O acesso por parte do PSIP pode dar-se mediante diferentes procedimentos e fica dependente da opção de *interface* que o PSPGC adote. Sobre esta matéria *vide infra* 4.2.

[33] No sentido da existência de um acordo prévio entre o PSIP e o comerciante, *vide* FRANCISCO MENDES CORREIA, "Uma revolução permanente? A DSP 2...", cit., p. 396. A existência de uma relação contratual entre o PSIP e o beneficiário é necessária para que este sirva de intermediário entre a conta do adquirente e a página do beneficiário. Este último necessita de facultar as informações necessárias (*v.g.* montante e identificador único de conta de pagamento) para que se possa executar a ordem de pagamento por conta do adquirente e em seu benefício. A mesma ideia é afirmada pela Federação Bancária Europeia em *Guidance for implementation of the revised Payment Services Directive – PSD2 Guidance,* 2.ª versão, 2019, disponível em https://www.ebf.eu (4.10.2020), p. 26, ao considerar que "*the definition of Payment Initiation Services (PIS) entails a contractual relationship between the PISP and the Merchant*".

[34] Segundo a al. ii) do art. 2.º, uma operação de pagamento pode consistir em depositar, transferir e levantar fundos. Pela natureza do serviço prestado pelo PSIP só estará em causa a iniciação de transferências eletrónicas de fundos. Neste âmbito, considerando a letra da lei no que contende com a definição e disciplina da atividade do PSIP, parece-nos que ao mesmo compete somente iniciar transferências a crédito, nos termos definidos pelo art. 2.º, al. ddd), impulsionadas pelo utilizador/devedor. A Comissão Europeia, nas Perguntas Frequentes sobre a DSP2, refere na questão n.º 18 e n.º 21, que o PSIP auxilia o utilizador a realizar transferências a crédito. *Vide* EUROPEAN COMMISSION, *Payment Services Directive: frequently asked questions,* Bruxelas, 2018, disponível em https://ec.europa.eu (1.10.2020).

[35] *Vide* TIAGO DA CUNHA PEREIRA, "DSP2: Oportunidades e Desafios", *in Revista de Direito Financeiro e dos Mercados de Capitais*, n.º 5, Vol. I, 2019, disponível em https://www.blook.pt/home (29.01.2020), p. 511.

[36] Quando os prestadores de serviços de iniciação de pagamentos prestam exclusivamente esse serviço, não podem deter fundos dos seus clientes. V. alínea a), do n.º 3, do art. 106.º.

qualquer tipo de controlo jurídico ou regulatório, dada a exclusão destes serviços pelo regime. Estas entidades acediam às contas através das *interface*s que o PSPGC oferece aos seus utilizadores para aceder à conta *online*, como se do utilizador se tratasse, o que levantava dúvidas sobre a licitude de tal acesso[37]. Hoje, a al. d), do n.º 3, do art. 106.º, exige que o PSIP se identifique como tal, de modo a garantir maior segurança no acesso, auxiliando o controlo do risco de interceção por partes não autorizadas aquando da comunicação estabelecida para efeitos de pagamento[38]. Porém, como determina o n.º 5 do referido artigo, não é pressuposto da permissão a existência de uma relação contratual entre os prestadores, encontrando-se o PSPGC obrigado a permitir o acesso numa base objetiva, não discriminatória e proporcionada, reservando-se, somente, à faculdade de o recusar por "motivos objetivamente justificados" perante o Banco de Portugal[39]. Apesar disso, o PSPGC tem de estar seguro sobre o acesso pelo terceiro prestador, pelo que, nos termos do disposto no art. 109.º, n.º 1, a recusa poderá ligar-se ao acesso fraudulento ou não autorizado à conta de pagamento por parte do PSIP, devendo reportar tal incidente ao Banco de Portugal.

A não exigência de uma relação contratual entre os prestadores de serviço envolvidos surge como decorrência da imposição de uma obrigação de não discriminação, que sobre os PSPGC recai e que tem como objetivo eliminar quaisquer barreiras ao acesso de novos terceiros prestadores às contas, encorajando a participação de entidades cada vez mais inovadoras no mercado interno de pagamentos. Considerando a conjuntura existente à data da publicação da DSP2 e a posição dominante que os bancos detinham sobre o mercado de serviços de pagamento, estes não possuíam incentivos suficientes para partilhar dados dos seus clientes. Ainda assim, tal circunstância não deixa de configurar um fator de risco na proteção da conta e dos dados do utilizador, na medida em que prescinde da necessidade dos prestadores acordarem, minuciosamente, os moldes e extensão da responsabilidade de cada um, não só referente à prevenção de operações não autorizadas, mas também, no que concerne com o tratamento de dados e a segurança das credenciais de segurança personalizadas. A letra da lei não excluiu a possibilidade da celebração de acordos, desde que tal não configure um pressuposto sem o qual o terceiro prestador não possa aceder à conta de pagamento[40].

Uma das principais preocupações que esta abertura acarreta, liga-se com a necessidade de garantir o carácter limitado do acesso às contas de pagamento por parte de terceiras entidades, para que não se desvirtue o esforço desenvolvido pela nova legislação no sentido de reforçar a segurança nas transações, que configura um pressuposto essencial à confiança dos consumidores nos novos serviços de pagamento. De modo a atenuar o contraste que o acesso à conta de pagamento cria em contraposição com as obrigações do utilizador e do

[37] FRANCISCO MENDES CORREIA, "DSP 2 e Normas Abertas de Comunicação Comuns e Seguras", *in Fintech II: Novos Estudos sobre Tecnologia Financeira*, CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Coord.), Coimbra, Edições Almedina, 2019, p. 158.
[38] O RSP vem estabelecer novas regras de repartição da responsabilidade por operações não autorizadas entre o PSPGC e o PSIP. *Vide infra* 3.3.
[39] V. arts. 69.º n.º 1 e 109.º.
[40] V. arts. 106.º, n.º 5 e 107.º, n.º 4. No sentido de que uma relação contratual pode existir entre os prestadores, surge a possibilidade do PSPGC e os serviços de informação sobre contas acordarem um número de vezes de acesso à conta de pagamento superior ao previsto na lei para cada período de 24 horas, por força do disposto na al. b), do n.º 5, do art. 36.º, do Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de novembro.

PSPGC em relação à segurança dos instrumentos de pagamento, o art. 106.º, n.º 3, al. e), ordena que o PSIP não possa conservar as credenciais de segurança personalizadas, uma vez que ao mesmo não é lícito armazenar dados de pagamento sensíveis, o que nos indica que as mesmas deverão ser eliminadas logo após a iniciação da ordem de pagamento e solicitadas novamente aquando cada operação em que o utilizador decida recorrer ao mesmo PSIP, mesmo que tenha sido celebrado um contrato-quadro[41].

1.3. O acesso à atividade

A prestação de serviços de iniciação de pagamentos só poderá dar-se por instituições devidamente autorizadas pelo Banco de Portugal. No que às instituições de pagamento concerne[42], o pedido de autorização requer um denso conjunto de requisitos que visam garantir a idoneidade das entidades para prestar serviços que assumem uma importante centralidade na vida dos utilizadores. Posto isto, destaca-se dos requisitos plasmados no art. 19.º, n.º 2, a alínea o), que exige o desenvolvimento de uma política de segurança que deverá incluir uma "avaliação pormenorizada dos riscos relacionados com os seus serviços de pagamento", bem como uma "descrição das medidas de controlo da segurança e de redução dos riscos tomadas" com vista à proteção do utilizador contra a fraude e utilização ilícita de dados. O n.º 6 do mesmo artigo, exige que o prestador, enquanto instituição de pagamento e que pretenda prestar apenas serviços de iniciação de pagamentos, subscreva um seguro de responsabilidade civil profissional ou garantia equivalente que tenha capacidade de cobrir os custos com um eventual reembolso do utilizador e do PSPGC em caso de operações não autorizadas. Por sua vez, o prestador só poderá iniciar a sua atividade quando estiver devidamente registado no registo público junto do Banco de Portugal, que deverá especificar os serviços prestados. Como reforço da proteção, esta circunstância deverá ser informada à Autoridade Bancária Europeia (EBA), de modo a que esta possa incluir o prestador no registo eletrónico central que visa registar todas as instituições de pagamento autorizadas na União Europeia[43].

2. O contrato de prestação de serviços de iniciação de pagamentos

[41] A al. k), do art. 2.º, engloba no conceito de dados de pagamento sensíveis as credenciais de segurança personalizadas e quaisquer dados que permitem a consumação de condutas fraudulentas. Será assim de se incluir, quaisquer elementos e dados utilizados para a autenticação forte do utilizador. Sobre a autenticação do utilizador, *vide infra* 3.1.
[42] A prestação de serviços de pagamento é, com predominância, efetuada por instituições de crédito, mas referirmo-nos apenas às instituições de pagamento, uma vez que o registo enquanto instituição de crédito está sujeita a regime diverso. Do mesmo modo, a autorização deverá ser requerida por instituições com sede em Portugal.
[43] V. art. 15.º da DSP2.

A entrada em vigor da DSP veio aclarar o entendimento do contrato de prestação de serviços de pagamento ou de utilização de um instrumento de pagamento enquanto um contrato-quadro. Como já vinha defendendo alguma doutrina portuguesa[44], desde a DSP que o contrato de utilização de um instrumento de pagamento é definido como o contrato-quadro que corresponde a "um contrato de prestação de serviços de pagamento que rege a execução futura de operações de pagamento individuais e sucessivas e que pode enunciar as obrigações e condições para a abertura de uma conta de pagamento"[45]. Porém, tal como entende Maria Raquel Guimarães, o contributo da Diretiva não foi suficiente para esclarecer se o contrato de utilização configura uma estrutura complexa contratual que prepara a celebração de outros contratos ou um único contrato de execução continuada e sucessiva, não fazendo de imediato denotar que na "execução futura de operações de pagamento" se dá a celebração de novos e autónomos contratos de execução de um contrato base[46].

A doutrina que, entre nós, considera que este contrato-quadro de utilização configura um único contrato de execução continuada, assenta a sua posição na obrigação, prevista no art. 120.º, n.º 1, do prestador do serviço executar a ordem de pagamento emitida pelo utilizador, considerando que as partes estariam desde logo vinculadas a um conjunto fixo de obrigações, consistindo a operação num mero ato de execução, ao qual o prestador já não se pode desvincular unilateralmente[47]. Por sua vez, o contrato-quadro exige a renovação da vontade das partes, mas concede liberdade às mesmas de incluir uma obrigação de contratar no futuro[48]. Por outro lado, o próprio RSP prevê a possibilidade do prestador se recusar a executar a operação no caso de não estarem preenchidas as condições previstas no contrato-quadro. Assim, afigura-nos que um mero ato de execução de um contrato já celebrado não é facilmente compatível com a possibilidade das partes não desencadearem a realização futura de nenhuma operação de pagamento, nem consegue justificar a falta de determinação de elementos essenciais dessa execução, isto é, o momento, o beneficiário e o montante da transferência. Tal circunstância, apesar de desvirtuar a verdadeira razão de ser de um contrato de utilização

---

[44] *Vide* MARIA RAQUEL GUIMARÃES, "El pago mediante tarjetas de crédito en el comercio electrónico. Algunos problemas relativos a su naturaleza jurídica, marco contractual y régimen aplicable, desde una perspectiva comparada en los Derechos portugués, español y comunitario" (tradução de DOMÍNGUEZ LUELMO, Andrés), *in Los medios electrónicos de pago — Problemas jurídicos*, MATA Y MARTÍN, Ricardo M. (dir.) / JAVATO MARTÍN, Antonio Mª, (coord.), Granada, Editorial Comares, 2007, pp. 183-186. Para mais desenvolvimentos sobre o tema, *vide* MARIA RAQUEL GUIMARÃES, *O Contrato-Quadro no Âmbito da Utilização de Meios de Pagamento Eletrónicos,* Coimbra, Wolters Kluwer/Coimbra Editora, 2011.

[45] V. art. 2.º, al. i).

[46] MARIA RAQUEL GUIMARÃES, *O Contrato-Quadro...,* cit., p. 553-556. Como defende a Autora, o contrato-quadro vem estabelecer a base de uma relação que tende a prolatar-se no tempo, definindo num momento inicial os traços gerais da relação, mas onde não esgota toda a sua complexidade. Deste modo, pressupõe a celebração de subsequentes contratos de execução cujos moldes vêm já determinados no primeiro encontro de vontades. É certo que, os contratos de aplicação dependem do contrato-base, mas o seu conteúdo não se mistura inteiramente com o deste, não configurando uma mera e automática execução do mesmo, uma vez que possui autonomia normativa na relação em que surge e, por isso, exige uma nova manifestação de vontade. Nas palavras da Autora, o contrato-quadro "pressupõe, portanto (pelo menos) dois momentos distintos em que ocorre a troca de consentimentos entre os contraentes. Existe necessariamente um "duplo consentimento" que marca a autonomia entre os diferentes contratos que compõem o conjunto". Para a Autora, o contrato de utilização de um instrumento de pagamento configura um contrato-quadro, *vide* MARIA RAQUEL GUIMARÃES, "Os Contratos-Quadro de Prestação de Serviços de Pagamento", *in I Congresso de Direito do Consumo*, CARVALHO, Jorge Morais (Coord.), Coimbra, Edições Almedina, 2016, 177-188.

[47] Entre nós, a considerar a existência de um único contrato de execução continuada, *vide* FRANCISCO MENDES CORREIA, *Moeda Bancária e Cumprimento*, Coimbra, Edições Almedina, 2017, pp. 618-628, em particular, nota de rodapé n.º 1672.

[48] MARIA RAQUEL GUIMARÃES, *O Contrato-Quadro...,* cit. pp. 64-65.

de um serviço ou instrumento de pagamento, não é inconcebível e encontra no contrato-quadro uma maior adequação, ao ceder margem de manobra às partes. A relação duradoura e complexa que normalmente se inicia, requer uma elasticidade contratual que só o contrato-quadro consegue facultar, mesmo com exigências acrescidas para umas das partes, justificadas na lei pela importância que os serviços de pagamento têm na vida dos consumidores.

Este percurso leva-nos à reflexão sobre a conceção da relação jurídica que se encontra por detrás da prestação dos novos serviços de iniciação de pagamentos[49]. A prestação desses serviços pode surgir a coberto de um contrato-quadro ou mediante um contrato de prestação de serviço de pagamento de carácter isolado, sendo que, no primeiro caso, o PSIP vincula-se à iniciação futura de pagamentos e no segundo, obriga-se a iniciar somente uma operação de pagamento.

Ao contrário do que se sucede com os serviços de pagamento em geral, o RSP enquadra, especificamente, as informações a disponibilizar aquando da prestação dos serviços de iniciação, na secção que regula as operações de pagamento de carácter isolado[50]. Esta circunstância parece ir no sentido de que o regime tende a considerar que os serviços serão prestados essencialmente mediante um contrato de prestação de serviço de pagamento de carácter isolado. A este propósito, o Banco Central Europeu, no seu parecer sobre a Proposta da DSP2, fez, precisamente, referência à possibilidade da existência de uma relação meramente pontual entre o prestador e o utilizador no caso dos serviços de iniciação[51]. Apesar da opção de sistematização da lei, não nos parece obstar que entre o PSIP e o utilizador se celebre um contrato-quadro que estipule as regras e condições que irão reger as futuras iniciações de pagamentos[52], uma vez que é o que melhor se coaduna com o objetivo da nova legislação em preencher o vazio jurídico que se verificava em relação a estes serviços[53]. De outro modo, estar-se-ia a restringir a forma como estes prestadores podem contratar com os utilizadores, bem como a não acompanhar a realidade que com maior frequência se verifica

[49] No nosso estudo iremos cingir-nos unicamente à relação contratual estabelecida entre o utilizador e o PSIP, deixando de fora a consideração sobre a relação que existirá entre o beneficiário e o PSIP, nomeadamente, através da celebração de um contrato em termos semelhantes ao da admissão de um meio de pagamento.
[50] Cfr. arts. 84.º, n.º 2, 85.º e 86.º. A matéria sobre a transparência das condições e requisitos de informação aplicáveis aos serviços de pagamento encontra-se plasmada no Capítulo II do Título III, dedicando-se as Secções II e III, designadamente, para as operações de carácter isolado e para as operações abrangidas por um contrato-quadro.
[51] *Vide* BANCO CENTRAL EUROPEU, Parecer do Banco Central Europeu de 5 de fevereiro de 2014 sobre uma proposta de Diretiva do Parlamento Europeu e do Conselho relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2013/36/UE e 2009/110/CE e revoga a Diretiva 2007/64/CE, CON/2014/9, Frankfurt, 2014, disponível em https://www.ecb.europa.eu (25.10.2019), explicação da Alteração n.º 27. A Proposta de Diretiva já inseria as informações a prestar no capítulo das operações de carácter isolado, opção que não foi contestada ao longo do processo legislativo. Cfr. Capítulo 2 da Proposta de Diretiva do Parlamento Europeu e do Conselho relativa aos Serviços de Pagamento no Mercado Interno, que altera as Diretivas 2002/65/CE, 2013/36/CE e 2009/110/CE e revoga a Diretiva 2007/64/CE, COM(2013) 547 final, Bruxelas, 24.07.2013.
[52] A Federação Bancária Europeia, nas suas Orientações relativas à DSP2, considerou que entre o utilizador e o PSIP seria, provavelmente, estabelecido uma relação pontual, por contraposição à celebração de um contrato-quadro com os prestadores de serviços de informação sobre contas. Ainda assim, parece não afastar a possibilidade de as partes estarem vinculadas previamente à iniciação de futuras operações por força de um contrato-quadro, reconhecendo que as informações a prestar antes da celebração do mesmo foram atualizadas para abranger os novos serviços. *Vide* EUROPEAN BANKING FEDERATION, *Guidance for implementation…,* cit., pp. 37 e 39.
[53] *Vide* considerandos 4 e 6 da DSP2.

em sede dos serviços de pagamento[54], isto é, a celebração de um contrato que permite disponibilizar ao utilizador um serviço no qual confia, constantemente disponível e ao qual pode recorrer de forma simplificada.

Sucede que, tanto num caso como no outro, a celebração deste contrato de prestação de serviços de iniciação, quando prestado por um terceiro prestador, já não se enquadra numa relação negocial complexa, como é aquela estabelecida entre o banco e o seu cliente, seio onde predomina a prestação de serviços de pagamento e que se inicia com a celebração de um contrato de abertura de conta, pelo que não é expetável que se desenvolva, ao longo do tempo, com a mesma complexidade[55]. Nada obsta à prestação de serviços de iniciação pelas instituições de crédito, mesmo com quem o utilizador já possua uma relação prévia, pelo que nestes casos já estaremos perante um contrato que decorre e se insere na complexa relação bancária, a par do que acontece com outros contratos de prestação de serviços de pagamento, como é o caso de utilização de cartão e de *homebanking*. Porém, surge-nos mais pertinente analisar a relação jurídica estabelecida entre o utilizador e o prestador quando este configura um terceiro face à relação que o utilizador possui com o banco que lhe gere a conta, por tal situação ser dotada de maior novidade e particularidade.

À complexa delegação de pagamento[56] que pode existir entre um utilizador de um instrumento ou serviço de pagamento e o prestador desse serviço, junta-se um novo interveniente que intercetará a operação num momento anterior à sua execução, ou seja, previamente à substituição do utilizador – o devedor – pelo seu banco. Assim, o prestador do serviço de iniciação irá, por conta do utilizador, aceder à conta de pagamento deste, domiciliada noutro prestador de serviço, para emitir uma ordem de pagamento. A concretização da iniciação de uma operação pressupõe que compita ao PSIP transmitir o consentimento do utilizador e emitir a ordem de pagamento, dois aspetos fulcrais no esquema das transações eletrónicas. A autorização da operação e a ordem de pagamento são aspetos diferentes, embora se possam mostrar coincidentes no mesmo ato nas transferências a crédito. Seguindo o entendimento de

[54] O considerando 57 da DSP2 reconhece que as operações abrangidas por um contrato-quadro são "de longe mais comuns e importantes de um ponto de vista económico". Acrescenta também que no caso de existir uma conta de pagamento ou um instrumento de pagamento específico será necessário um contrato-quadro. Nesta linha, a possibilidade de não existir a emissão de um instrumento de pagamento pelo PSIP poderá ajudar-nos a compreender a inserção sistemática das informações a prestar pelos mesmos na secção das operações de carácter isolado, sem que daí se retire a exclusividade desse modelo. Ainda assim, importa ter presente que o RSP define, na alínea aa), do art. 2.º, instrumento de pagamento como "um dispositivo personalizado ou conjunto de procedimentos acordados entre o utilizador e o prestador de serviços de pagamento e a que o utilizador de serviços de pagamento recorra para emitir uma ordem de pagamento", pelo que a ampla definição da lei permite que se considere existir, com frequência, a emissão de um instrumento pelos prestadores.

[55] Sobre a inserção do contrato de utilização de instrumentos ou serviços de pagamento na relação bancária geral, *vide* RAQUEL SOFIA RIBEIRO DE LIMA, "A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa", *in RED – Revista Eletrónica de Direito*, n.º 3, Porto, CIJE/FDUP, 2016, disponível em https://www.cije.up.pt/pt/red (20.10.2019), pp. 14-16. Para um maior desenvolvimento sobre esta inserção e a natureza da relação entre o banco e o seu cliente, *vide* MARIA RAQUEL GUIMARÃES, *O Contrato-Quadro...*, cit. pp. 345-381.

[56] Melhor ilustrando o esquema delegatório que sustenta a emissão e execução de uma operação de pagamento eletrónico, mas, em concreto, através da utilização de um cartão, *vide* MARIA RAQUEL GUIMARÃES, *O Contrato-Quadro...*, cit., pp. 383-427. A Autora defende que a operação configura uma delegação passiva, onde o utilizador – e primitivo devedor, – é substituído por um novo devedor, o banco, na relação com o beneficiário. ANTUNES VARELA define que a delegação "consiste na convenção pela qual uma pessoa (delegante) incumbe uma outra (delegado) de realizar certa prestação a terceiro (delegatário), que é autorizado a recebê-la em nome próprio", *vide* JOÃO DE MATOS ANTUNES VARELA, *Das Obrigações em Geral*, Vol. II, Almedina, 11.ª Reimp. da 7.ª Ed, Coimbra, Almedina, 2015, p. 370.

que entre o utilizador e o banco se formaliza um contrato base que prepara a celebração de novos contratos, o consentimento exigido no RSP para a execução de uma operação de pagamento eletrónico irá traduzir a renovação da manifestação de vontade do utilizador para a celebração de um concreto contrato em execução do acordo inicial. Como escreve Maria Raquel Guimarães, "os contratos de mandato em que se traduzem as ordens de pagamento emitidas pelo titular do cartão ao seu banco" e que "pressupõem, cada um deles, novas declarações negociais convergentes"[57], passam a poder ser celebrados por um terceiro, com o qual é celebrado um contrato de prestação de serviços na modalidade de mandato, onde o PSIP substituirá o utilizador na emissão das declarações negociais necessárias para a celebração do contrato de execução com o PSPGC, autorizando e emitindo a ordem de pagamento sob instrução do utilizador e por conta deste[58]. Tudo se desencadeará dentro dos termos e regras acordadas entre este e o PSPGC que disciplinam as operações de pagamento eletrónico[59]. Esta circunstância não deixa de nos fazer questionar se estamos perante um verdeiro mandato ou de uma prestação de serviços atípica, onde o PSIP assumiria o papel de núncio, a quem incumbe transmitir uma declaração de vontade já consumada, não sendo considerado um verdadeiro mandato por não se tratar da prática de atos jurídicos, mas de simples atos materiais [60]. É certo que, quando o utilizador autoriza o PSIP a iniciar a operação, o mesmo já determina, a início, em que moldes deverá ser a ordem emitida e em relação a quem. Ainda assim, não se deixa de notar certa autonomia do PSIP na emissão – e não transmissão – da declaração negocial, na medida em que este poderá abster-se de o fazer, nomeadamente quando não confirma a existência de fundos suficientes para a iniciar. De semelhante modo, sobre o mesmo recai um dever de gerir os riscos da sua atividade e das operações que inicia[61], pelo que deverá sempre aferir se há segurança para a iniciação da mesma[62]. Contrariamente, o mero transmitente da declaração necessita apenas de possuir capacidade de transmitir na medida em que não precisa de entender e querer em determinado sentido.

---

[57] *Vide* MARIA RAQUEL GUIMARÃES, *O Contrato-Quadro...*, cit., p. 510.
[58] Para quem considera que estamos perante um único contrato de execução continuada, a ordem de pagamento consiste na instrução que o mandante emite ao mandatário, nos termos do art. 1161.º, al. a), do Código Civil (CC), que passaria a ser dada pelo PSIP. *Vide* FRANCISCO MENDES CORREIA, *Moeda Bancária...*, cit., pp. 739-741.
[59] Salvaguardando o RSP o direito do utilizador recorrer aos serviços de iniciação, o banco não se poderá recusar a executar a operação como lhe era reconhecido nos termos do art. 771.º do CC.
[60] *Vide* LUÍS MANUEL TELES DE MENEZES LEITÃO, *Direito das Obrigações*, volume III, Coimbra, 12.ª Ed., Edições Almedina, 2018, p. 428. Para mais desenvolvimentos sobre a figura do núncio, mas contraposta à representação, *vide* CARLOS ALBERTO DA MOTA PINTO, *Teoria Geral do Direito Civil*, Coimbra, 2.ª Reimp. da 4.ª Ed., Coimbra Editora, 2012, pp. 543-544.
[61] *Vide infra* 2.1.
[62] Sobre a movimentação da conta por terceiros, *vide* M. JANUÁRIO DA COSTA GOMES, *Contratos Comerciais*, Coimbra, Edições Almedina, 2012, pp. 128-134. O Autor refere que o titular da conta pode conceder poderes representativos, mediante procuração, para a movimentação da sua conta. Neste seguimento, parece-nos que entre o PSIP e o utilizador deverá ser de existir um mandato com representação, agindo por conta do utilizador e em nome dele, de modo a que os efeitos se repercutem imediatamente na sua esfera. Parece-nos que é o que melhor se coaduna com a pessoalidade que normalmente se associa à prestação de um consentimento. Ainda assim, mesmo que o mandato seja considerado não representativo, estando em causa direitos de crédito sobre o PSPGC, os mesmos podem ser imediatamente exercidos pelo utilizador, nos termos do art. 1181.º, n.º 2, do CC, sem que exista a transferência desses direitos. Como entende MENEZES LEITÃO, nestas situações a lei prevê a tese da projeção imediata "segundo a qual os efeitos repercutem-se diretamente na esfera do mandante sem terem que passar pelo património do mandatário". *Vide* LUÍS MANUEL TELES DE MENEZES LEITÃO, *Direito das Obrigações*, cit., pp. 449 e 453.

Embora esta nova relação não surja diretamente como desenvolvimento da relação complexa estabelecida, não deixa de decorrer dela, uma vez que, para que o PSIP possa oferecer os seus serviços, é necessário que tenha existido um acordo de vontades prévio entre o utilizador e o outro prestador de serviços, através da celebração de um contrato para abertura da conta e de depósito ou abertura de crédito, uma vez que o PSIP só poderá iniciar uma operação se confirmar que o titular da conta possuí fundos disponíveis para movimentar. Para além disso, o mandato do PSIP está funcionalmente ligado à disponibilização da conta de pagamento em linha, pressupondo que entre o utilizador e o seu banco se tenha procedido à celebração de um contrato de utilização de *homebanking*, que configura também um contrato-quadro[63]. Assim, a liberdade de prestação por parte do PSIP é geneticamente dependente de um conjunto de contratos previamente celebrados entre os seus potenciais clientes e outros prestadores de serviços.

O processo inerente a esta prestação pressupõe que, num primeiro momento, convergem três partes distintas, o titular da conta e do instrumento, o PSIP e o PSPGC, em termos semelhantes à estrutura tripartida em que se desenvolve a execução de uma operação de pagamento eletrónico. Porém, tal não se basta para a concretização da finalidade única para que todos os intervenientes concorrem, exigindo que, à primeira estrutura, se coligue e se verifique outros três feixes relacionais[64], mas entre o PSIP, o banco do utilizador e o beneficiário, na medida em que o primeiro interage com o banco para emitir a ordem de pagamento, com o último para confirmar a existência de fundos e, noutro ponto polarizador, o banco perante o beneficiário, procedendo ao pagamento por conta do utilizador. Tudo se desenvolve como se, na habitual estrutura existente entre o utilizador, o seu banco e o comerciante, o primeiro passe a ser representado pelo PSIP, de onde nasce uma nova ramificação que se reparte, do mesmo modo, em três pólos distintos.

2.1. Os deveres do prestador de serviços

Em paralelo com as orientações seguidas pela União Europeia em matéria de proteção do consumidor, o RSP não se afasta do protagonismo concedido à informação pré-contratual a prestar por quem maior influência detém na relação contratual[65], estabelecendo-se a obrigação

[63] Sobre a noção do contrato de utilização de *homebanking* e a sua conceção como um contrato-quadro, *vide* CAROLINA FRANÇA BARREIRA, "Home banking: A Repartição dos prejuízos decorrentes de fraude informática", *in RED – Revista Eletrónica de Direito*, n.º 3, Porto, CIJE/FDUP, 2015, disponível em https://www.cije.up.pt/pt/red (20.10.2019), pp. 7-16. A Autora define o contrato de utilização de *homebanking* como "um serviço concedido pelas instituições bancárias aos seus clientes, permitindo-lhes executar uma série de operações bancárias, por telefone ou *online*, relativamente às contas de que sejam titulares".

[64] Quando nos referirmos à necessidade de concorrerem três partes distintas, em diferentes momentos, não nos podemos esquecer que entre o PSIP e o PSPGC poderá não existir um negócio jurídico.

[65] Em virtude da essencialidade e abrangência que os serviços de pagamento assumem na vida dos indivíduos, não se pode deixar de notar que a disciplina do RSP não se aplica somente às relações com consumidores, visando proteger os utilizadores quando atuam com objetivos ligados às suas atividades comerciais ou profissionais ou que não sejam pessoas singulares. Deste modo, os utilizadores dos serviços de pagamento podem, ou não, ser consumidores, segundo a aceção da Lei da Defesa do Consumidor (Lei n.º 24/96, de 31 de junho). Sucede que, várias obrigações que incidem sobre o PSP podem ser afastadas pelas partes quando o utilizador não é um consumidor, como acontece com os requisitos de informação previsto no Capítulo II do Título III, por força do

do PSP dispor, antes do utilizador ficar vinculado, "de forma facilmente acessível, as informações e condições especificas" dos serviços a prestar[66]. De modo a proteger a posição do consumidor e os demais utilizadores que eventualmente se deparem com consequências atinentes à falta ou deficiência de informação necessária sobre os serviços, cabe ao PSP provar que cumpriu os requisitos de informação[67].

Para além da previsão específica de um conjunto de deveres de informação no RSP, o PSIP sempre estará vinculado a outros deveres que decorrem das regras e princípios gerais como é o caso do princípio da boa-fé que deverá pautar a conduta das partes na fase pré-contratual e na execução do contrato, por força dos arts. 227.º e 762.º, n.º 2, ambos do CC[68].

O PSIP deverá fornecer de forma clara e detalhada a informação essencial para a sua correta identificação junto do utilizador antes de proceder à emissão da ordem de pagamento[69] e da vinculação a um contrato. Já no que concerne com informações contratuais, o PSIP deve, após a iniciação da ordem, confirmar junto do ordenante que a mesma foi bem-sucedida e disponibilizar uma referência que identifique a operação de pagamento e as informações transmitidas com aquela, devendo fornecer ao PSPGC idêntica referência[70]. Nas informações prestadas deverá constar o montante da operação de pagamento que, por sua vez, não é suscetível de ser alterado por parte do PSIP, nem qualquer outro elemento da operação que tenha sido definido pelo utilizador e/ou pelo prestador de serviços que gere a sua conta[71]. O regime não exclui a possibilidade do PSIP cobrar encargos diretamente ao utilizador pela usufruição dos seus serviços, devendo, por força da al. d), do art. 85.º, informar o ordenante, após a iniciação, do montante discriminado dos encargos a pagar pelo serviço prestado. Como tal informação, pela sua natureza, deveria ser fornecida antes da vinculação, o Banco de Portugal impõe que os encargos cobrados aos utilizadores dos serviços de pagamento sejam previamente informados a estes, nomeadamente, através da adequada divulgação do preçário, ainda que tais serviços sejam prestados pela internet[72].

Uma informação que se mostra imprescindível na prestação destes serviços é a consciencialização do utilizador sobre as medidas que deve tomar para preservar a segurança

n.º 3, do art. 76.º. Para aplicação desta matéria, as microempresas equiparam-se a consumidores. Previsão semelhante encontra-se em sede de direitos e obrigações relativas à prestação e utilização dos serviços, *vide* art. 100.º, n.º 2. Prevê-se igualmente exceções para instrumentos de pagamento que digam respeito a operações de pagamento de baixo valor nos arts. 81.º e 102.º.

[66] V. art. 78.º, al. b) e art. 83.º, n.º 1, especificamente para as operações de carácter isolado, e o art. 91.º para as operações abrangidas por um contrato-quadro.

[67] Considerando a natureza dos contratos celebrados no âmbito dos serviços de pagamento, é também de se aplicar o regime da Cláusulas Contratuais Gerais, vertido no Decreto-Lei n.º 446/85, de 25 de outubro, que igualmente prevê especiais deveres de comunicação e informação, sendo aqui de se aplicar o disposto nas al. a) e b), do art. 8.º, do referido diploma, considerando-se como excluídas todas as cláusulas que não sejam comunicadas e devidamente informadas ao utilizador.

[68] Uma vez que se trata de um contrato celebrado à distância com um consumidor, o PSIP está vinculado aos deveres pré-contratuais constantes do Decreto-Lei n.º 95/2006, de 29 de maio, que estabelece o regime jurídico aplicável aos contratos à distância relativos a serviços financeiros, pelo que no conceito de serviço financeiros definido pelo diploma é de se incluir os serviços de pagamento. O mesmo prevê um direito de livre resolução que terá certas dificuldades de articulação com o imediatismo do serviço no caso de operações de carácter isolado. *Vide* FRANCISCO MENDES CORREIA, *Moeda Bancária...*, cit., pp. 680-681.

[69] V. art. 84.º, n.º 2.

[70] V. art. 85.º, al. a) e b) e art. 86.º.

[71] V. art. 106.º, n.º 3, al. h).

[72] A exigência de informação prévia dos encargos cobrados ao utilizador decorre do Aviso do Banco de Portugal n.º 8/2009, aplicável também às instituições de pagamento por força do Aviso do Banco de Portugal n.º 2/2021.

da sua conta de *homebanking* ou de qualquer outro instrumento de pagamento que o PSIP lhe faculte para iniciar os pagamentos. Este dever só surge no âmbito de um contrato-quadro na medida em que se espera que a relação perdure e novas operações sejam iniciadas pelo prestador, mas não deixa de ser necessário acautelar o utilizador nas operações isoladas[73], principalmente perante as situações de *phishing* que podem ocorrer depois da prestação do serviço[74]. Surgem-nos insuficientes, as informações a prestar ao utilizador no caso de celebração de um contrato de prestação de serviços de pagamento de carácter isolado, na medida em que o utilizador poderá não saber que, após a iniciação, o prestador deixa de lhe poder exigir qualquer outra informação sobre a sua conta.

O dever principal do PSIP consiste precisamente na iniciação da operação, que inclui, como já se disse, a autorização e a emissão da ordem de pagamento. Para além disso, a iniciação deverá ser executada devidamente e conforme o instruído pelo utilizador, sob pena do prestador vir a ser responsável, nos termos do art. 132.º.

A lei sujeita o PSIP a dois importantes deveres em matéria de segurança e confidencialidade, o dever de gestão de riscos operacionais e de segurança e o dever de segredo profissional. Em relação ao primeiro, o PSIP vê-se obrigado a estabelecer "um quadro com medidas de mitigação e mecanismos de controlo adequados", que lhes deverá permitir gerir, detetar e classificar incidentes, bem como comunicar qualquer incidente de carácter severo[75]. Por força deste dever, parece-nos que deverá ser legítimo ao PSIP recusar a prática de qualquer ato quando tenha fortes suspeitas de que a operação a realizar seja fraudulenta ou insegura, com vista a evitar o prejuízo na conta do utilizador. No que contende com o dever de segredo profissional, o RSP prevê que o PSIP, registado enquanto instituição de pagamento, se encontre vinculado ao mesmo dever de segredo[76] previsto para as instituições de crédito, remetendo expressamente para os arts. 78.º e 79.º do Regime Geral das Instituições de Crédito e Sociedades Financeiras (RGICSF), pelo que terá de assegurar que as informações sobre factos ou elementos respeitantes às relações com o utilizador permaneçam em sigilo entre todas as pessoas envolvidas na sua atividade, quer a título ocasional ou permanente. A

[73] O n.º 3, do art. 84.º, prevê que outras informações especificadas para as operações de pagamento abrangidas por um contrato-quadro possam ser fornecidas quando "aplicável" e se mostre pertinente às operações de carácter isolado.

[74] O *phishing* pode ser definido como uma fraude eletrónica que visa obter dados relativos a instrumentos de pagamento mediante mensagens de correio eletrónico onde se arroga a identidade de uma determinada instituição e que, por avisos referentes à ocorrência de uma operação, a solicitar a retificação da mesma ou por uma geral necessidade de dados, tenta aliciar o utilizador a facultá-los diretamente. *Vide* MARIA RAQUEL GUIMARÃES, "O phishing de dados bancários e o pharming de contas. Análise jurisprudencial", *in III Congresso de Direito Bancário*, VASCONCELOS, L. Miguel Pestana de (Coord.), Coimbra, Edições Almedina, 2018, pp. 418-422. No caso de ser feita referência a prestadores com quem o utilizador possa possuir uma relação ou ter contratado isoladamente, este pode ser levado a crer que deverá disponibilizar novamente os seus dados. Os bancos tendem a avisar os utilizadores desses riscos na sua página de *homebanking*, alertando que não exigem dados por mensagem, por exemplo. Semelhante cautela é necessária também na utilização de serviços de iniciação, pelo que, tal informação deveria sempre constar e não depender unicamente da prudência de cada prestador em concreto.

[75] V. art. 70.º e 71.º. O Banco de Portugal na Instrução n.º 1/2019 sobre o reporte de incidentes de carácter severo, veio defini-los como "um evento único ou uma série de eventos conexos e não previstos pelo PSP, que tem, ou poderá vir a ter, um impacto adverso na integridade, disponibilidade, confidencialidade, autenticidade e/ou continuidade dos serviços relacionados com pagamentos".

[76] Cfr. art. 16.º.

violação desse dever pelo PSIP pode consubstanciar num crime de violação de segredo previsto no art. 195.º do Código Penal.

2.2. O consentimento para execução de operações de pagamento e o consentimento para a recolha e tratamento de dados

Como sucedia anteriormente, uma operação de pagamento necessita da autorização do ordenante[77] e tal só acontece quando o mesmo consente na sua execução, de modo a que o PSP se substitua na realização do pagamento a que o primeiro está adstrito. De acordo com o disposto no art. 103.º, cada operação de pagamento tem de ser precedida pelo consentimento do utilizador, prestado na forma acordada pelas partes, existindo na maioria das vezes, uma coincidência entre a autenticação e o consentimento[78].

Uma das novidades a este respeito contende com a possibilidade de o utilizador poder prestar o seu consentimento por intermédio de outra pessoa, onde protagonizam os serviços de iniciação. É o que prevê, precisamente, o n.º 4 do artigo supracitado. Isto diz-nos que a autorização da execução da operação deixa de ser feita, todas as vezes, diretamente e na pessoa do utilizador. A par disso, uma questão delicada trazida pelo RSP contende com o sentido do "consentimento expresso" do utilizador que não recebe qualquer definição legal. O conceito é introduzido, desde logo, no art. 106.º, n.º 2 e no art. 107.º, n.º 2, al. a), relativos à prestação dos serviços pelo PSIP e PSIC e ao acesso à conta de pagamento pelos mesmos.

[77] Como se verificava no regime anterior, a lei refere-se ao ordenante como aquele que ordena ao prestador a execução de uma operação de pagamento. Porém, quando nos referirmos a ordenante no âmbito da autorização de uma operação, fazemo-lo no sentido de quem tem legitimidade para o fazer, dado que, nas operações não autorizadas, com exceção das que se dão por erro técnico do PSP, não deixa de existir um ordenante, estranho à relação estabelecida e que não obteve o consentimento do utilizador para iniciar uma ordem de pagamento em relação à aquela conta. O beneficiário também assume o papel de ordenante numa transferência a débito, porém, é referido no RSP sempre como beneficiário em contraposição do titular da conta ordenante. Não concordando com o termo empregado, *vide* MARIA RAQUEL GUIMARÃES, "The debit and credit card framework contract and its influence on European legislative initiatives", *in InDret Comparado, Revista para el Análisis del Derecho*, n.º 2, 2012, disponível em http://www.indret.com/es (24.09.2020), p. 13. No mesmo sentido, *vide* RITA MAFALDA VERA-CRUZ PINTO BAIRROS, "A transferência a crédito...", cit., p. 285, nota de rodapé 182 e PATRÍCIA GUERRA, "A realização de operações de pagamento não autorizadas e a tutela do utilizador de serviços de pagamento em face do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica", *in RED - Revista Eletrónica de Direito*, n.º 2, Porto, CIJE/FDUP, 2016, disponível em https://www.cije.up.pt/pt/red (27.09.2019), p. 27, nota de rodapé 98.

[78] Sobre a possível coincidência entre a autenticação e o consentimento, veja-se o exemplo ilustrado por MARIA RAQUEL GUIMARÃES em "(Ainda) a responsabilidade pelo uso indevido de instrumentos de pagamento eletrónicos em operações presenciais e à distância", *in I Congresso de Direito Bancário*, VASCONCELOS, L. Miguel Pestana de (Coord.), Coimbra, Edições Almedina, 2015, p. 123. A Autora refere que a autorização da operação dá-se mediante a adoção, por parte do utilizador, dos comportamentos fixados no contrato para o efeito, tais como a "marcação de um código secreto num terminal de um computador instalado no estabelecimento do beneficiário, assinatura manual, inserção de uma ou mais chaves de acesso no site do banco, [...], no caso do *homebanking*". O último caso, cada vez mais atual, ilustra de forma pragmática a coincidência que poderá existir entre o consentimento e a autenticação do utilizador, de tal modo que as situações de operações não autorizadas que se verificam nesta sede surgem associadas à apropriação indevida das credenciais de segurança personalizadas que o utilizador se serve para se autenticar na página *online* do banco. Ainda assim, não se pode considerar em absoluto que o consentimento apenas se pode obter através da autenticação do utilizador, uma vez que a autenticação, embora possa carregar consigo o consentimento necessário para autorizar a operação, consiste, antes, de acordo com o definido pelo RSP no art. 2.º, al. *c*), num "procedimento que permite ao prestador de serviços de pagamento verificar a identidade de um utilizador de serviços de pagamento ou a validade da utilização de um instrumento de pagamento específico, incluindo a utilização das credenciais de segurança personalizadas do utilizador". O objetivo é verificar a identidade e legitimidade do utilizador, isto é, apurar se o utilizador é igualmente o titular da conta, e não, sem mais, a exteriorização do consentimento exigido para autorizar uma operação.

O conceito surge novamente no art. 136.º, n.º 3, que determina, em matéria de proteção de dados pessoais[79], a exigência do consentimento expresso do utilizador para o acesso aos seus dados e, consequentemente, à conta de pagamento onde constam esses dados no caso de terceiros prestadores[80]. Certo é que o conceito de consentimento expresso do utilizador, surge sempre associado aos serviços dos terceiros prestadores e ao tratamento de dados. Sobre esta matéria, entendeu a Organização Europeia de Consumidores (BEUC) que se deve distinguir entre consentimento simples, que é exigido para a autorização das operações de pagamento nos termos do art. 103.º, e consentimento expresso, referido para o acesso à conta e aos dados pessoais do utilizador[81] por parte de terceiros prestadores[82]. Este último deverá ser, no entendimento da BEUC, interpretado à luz da definição de consentimento para tratamento de dados pessoais[83], ao abrigo do Regulamento Geral sobre a Proteção de Dados (RGPD). Esta ideia é sustentada com base na estipulação no art. 136.º e pela omissão da DSP2 em definir especificamente em que consiste ou como deverá manifestar-se o referido consentimento[84].

Ainda que se denote a clara distinção da formulação feita pelo legislador nos preceitos em análise e se compreenda a posição adotada pela BEUC, não nos parece que o consentimento

[79] Para o nosso estudo importa ter presente em que consiste dados pessoais. Segundo a definição do art. 4.º, 1), do Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE, *in JO L 119 de 4.5.2016*), serão dados pessoais quaisquer informações relativas a uma pessoa singular identificada ou identificável. Acrescenta que uma pessoa é identificável quando possa ser identificada por referência a "nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular". Assim, poderá revelar qualquer informação relativa à vida privada, profissional e social de uma pessoa que abrange aspetos referentes à mesma. Essa informação tem de permitir identificar um sujeito e pode abranger tanto dados objetivos como subjetivos. Sobre o conceito de dados pessoais, *vide* A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019*, Coimbra, Edições Almedina, 2020, pp. 107-112 e 120-129. Posto isto, quaisquer informações referentes à conta de pagamento do utilizador, como o nome do titular, o IBAN, as transações realizadas, bem como a localização do IP do utilizador na utilização do serviço de iniciação, podem ser considerados dados pessoais. Pela iniciação de operações, o PSIP consegue descortinar e avaliar hábitos de consumo daquele concreto utilizador.

[80] Atenta-se que a referência feita no art. 136.º, n.º 3, engloba todos os prestadores de serviços de pagamento e não somente os terceiros prestadores.

[81] Recorda-se que o utilizador dos serviços de pagamento pode ser, de acordo com a al. *ee*), do art. 2.º, uma pessoa singular ou coletiva que utiliza um serviço de pagamento. Diferentemente, o titular de dados pessoais só poderá ser uma pessoa singular identificada ou identificável. Por sua vez, ambas as legislações se aplicam quer a consumidores quer a pessoas que atuem profissionalmente, embora o RSP prevê aspetos especiais para consumidores. Posto isto, a questão sobre a interação do RSP e o do RGPD, em matéria de proteção do utilizador, só poderá ter relevância quando o mesmo configure uma pessoa singular.

[82] THE EUROPEAN CONSUMER ORGANISATION, *BEUC's Recommendations to the EDPB on the interplay between the GDPR and PSD2,* BEUC-X-2019-021, Bruxelas, 2019, disponível em https://www.beuc.eu (23.11.2019), p. 3.

[83] Nos termos da ampla definição do art. 4.º, n.º 2, do RGPD, é de se considerar tratamento de dados a sua recolha, a consulta, a utilização, a conservação, o apagamento e a destruição, pelo que não é difícil notar que no desenvolvimento das atividades dos prestadores de pagamento, os mesmos procedam a várias operações de tratamento enquanto responsáveis por determinar as finalidades e os meios de tratamento de dados pessoais. Cfr. art. 4.º, 7), do RGPD.

[84] No mesmo sentido e interpretando o consentimento referido no RSP à luz da definição de consentimento para tratamento de dados pessoais previsto no RGPD *vide* TIAGO CORREIA MOREIRA; INÊS ANTAS DE BARROS; ISABELA ORNELAS, "Partilha de dados pessoais...", cit., pp. 155-156. O RGPD exige que o consentimento necessário para o tratamento dos dados nos termos da al. a), n.º 1, do art. 6.º, do RGPD, consista numa manifestação de vontade livre, específica, informada e inequívoca. Note-se que até março de 2021, a versão portuguesa do RGPD exigia no art. 4.º, 11), uma vontade explícita, por contraposição à versão inglesa, espanhola, francesa e italiana do mesmo, que faziam menção à manifestação de uma vontade inequívoca através de uma declaração ou ato positivo. Na proposta do texto do RGPD encontrava-se a referência ao consentimento explícito, opção que foi afastada na versão final com o objetivo de desviar a possibilidade de vir a ser interpretado como um consentimento escrito. O mesmo não aconteceu na versão portuguesa após a publicação do diploma, dificultando, nos últimos anos, a diferença entre o consentimento para o tratamento de dados pessoais em geral e o tratamento de dados sensíveis com base no consentimento previsto na al. a), do n.º 2, do art. 9.º, do RGPD, que deverá ser explícito. Esta divergência foi finalmente retificada na versão portuguesa do diploma, cingindo-se o termo explícito apenas às categorias especiais de dados pessoais.

expresso referido no RSP pressuponha a interpretação do mesmo à luz do RGPD. O n.º 2, do art. 106.º, estabelece que "quando o ordenante der o seu consentimento expresso para a execução de um pagamento nos termos do artigo 103.º", parece logo indiciar que a referência ao consentimento expresso equivale ao consentimento estabelecido no art. 103.º, para a autorização das operações de pagamento. Há que reconhecer alguma ambiguidade ao preceito do n.º 2, na medida em que suscita a dúvida sobre a quem o ordenante está a prestar o consentimento: ao prestador que gere a conta ou ao PSIP. A formulação parece indicar no sentido de se referir ao consentimento prestado ao PSPGC, de acordo com os termos do art. 103.º, n.º 1 e n.º 4. A particularidade, parece-nos, está no facto de o consentimento ser dado através do PSIP[85], pressupondo que tenha havido a solicitação por parte do utilizador de serviço de iniciação e com isto, a autorização para este iniciar a operação, também de acordo com o art. 103.º e o estabelecido no contrato celebrado. Embora seja feita a referência ao conceito "expresso", que não se encontra no art. 103.º, a remissão feita não poderá deixar de significar que o consentimento é feito nos termos do art. 103.º, ao abrigo da hipótese reconhecida no n.º 4 em relação ao PSPGC, que permite ao utilizador fornecer o seu consentimento mediante um PSIP. Deste modo, o preceito do n.º 2, do art. 106.º, só poderá referir-se ao consentimento que o PSPGC tem de receber para executar a operação de pagamento, mas por intermédio do PSIP, o que irá sempre pressupor a autorização prestada pelo ordenante para a iniciação do pagamento, justificando-se assim a sua inserção sistemática no art. 106.º e a vinculação aos deveres postulados no n.º 4, que contende essencialmente com a atuação do PSPGC perante o PSIP no momento da iniciação. Deste modo, parece-nos importante não confundir a natureza distinta do consentimento previsto no RSP e no RGPD, pelo que a revogação do consentimento prevista no n.º 3, do art. 7.º, do RGPD, nada tem a ver, nem choca, com o carácter irrevogável de uma ordem de pagamento previsto n.º 2, do art. 121.º do RSP.

Ainda assim, reconhece-se que o estabelecido no art. 136.º é claro em exigir o consentimento expresso do utilizador para o tratamento de quaisquer dados, mas não se compreende tal exigência, uma vez que na prestação de um serviço estará em causa a celebração e execução de um contrato, podendo configurar um contrato-quadro e sucessivos contratos de execução ou um contrato de prestação de serviços de pagamento de carácter isolado.

Se o prestador, terceiro face à relação do banco com o seu cliente, acede à conta de pagamento e, consequentemente, a certos dados referentes à mesma, fá-lo ao abrigo, e por necessidade, da execução de um contrato que o utilizador se dispôs a celebrar com o mesmo, ainda que no âmbito do comércio eletrónico. O tratamento de dados pessoais do utilizador necessários para a prestação de serviços de iniciação é lícito ao abrigo da al. b), do n.º 1, do art. 6.º do RGPD. O mesmo se poderá dizer em relação à necessidade da conservação dos dados relativos à operação efetuada ao abrigo da al. c) do mesmo preceito, na medida em que o PSIP tem de estar apto a conseguir provar que a operação foi devidamente autenticada, registada e que

[85] Neste caso, a forma de prestação do consentimento para autorizar uma operação já será através do recurso a um PSIP, isto é, através da intervenção de um terceiro, parecendo-nos que, neste caso, já não haverá uma necessária coincidência entre o consentimento e autenticação do utilizador.

não foi afetada por nenhuma avaria técnica ou deficiência do serviço prestado, por força do n.º 2, do art. 113.º[86]. Não poderia o prestador ficar dependente do consentimento expresso do utilizador para cumprir o que a lei lhe onera. Pelo exposto, é difícil de se compreender a exigência do n.º 3, do art. 136.º, a não ser no sentido de que a manifestação de um consentimento expresso deva ser compreendida como a necessidade, aquando da celebração do contrato, de consciencializar o utilizador de que está a autorizar o acesso à sua conta e aos seus dados[87].

Foi este o entendimento que o Comité Europeu para a Proteção de Dados (EDPB, acrónimo de *European Data Protection Board*) seguiu na sua carta à deputada do Parlamento Europeu Sophie in 't Veld, que levantava questões relativas à proteção de dados no âmbito da DSP2 e que foi confirmado, posteriormente, nas suas orientações relativas à articulação da DSP2 e do RGPD[88]. O EDPB considerou que o consentimento previsto no n.º 2, do art. 94.º, da DSP2, deverá ser tido como um requisito adicional de natureza contratual, configurando-o como um consentimento contratual, surgindo como reforço da posição do utilizador, mas que tal não se confunde com as bases de licitude do tratamento de dados no âmbito do RGPD, nem pode desvirtuar as regras plasmadas na legislação de proteção de dados[89]. Aponta para a importância de o titular dos dados ficar consciente dos propósitos para qual os mesmos são tratados, devendo tal informação ser destacada e explicitamente aceite pelo titular. Compreende-se que seja necessário, de modo a garantir uma plena conformidade com o RSP, que o prestador requeira do utilizador uma aceitação, concreta e separada das restantes cláusulas, do acesso à conta de pagamento e aos seus dados, de modo a garantir que o utilizador solicitou o serviço tendo plena consciência desse facto. Porém, do puro ponto de vista do RGPD, nada obstaria a uma aceitação generalizada das condições gerais do serviço, desde que ao utilizador seja fornecida a informação sobre a necessidade de tratamento dos seus dados pessoais relacionados com a conta de pagamento e para que finalidade específica[90].

Por outro lado, se se considerasse o disposto na legislação dos serviços de pagamento como uma cumulação, enquanto exigência acrescida, de duas bases legais para o tratamento lícito

---

[86] *Vide* TIAGO DA CUNHA PEREIRA, "DSP2: Oportunidades...", cit., p. 516-517.

[87] No mesmo sentido, *vide* DILJA HELGADOTTIR, "The interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players", *in Trinity College Law Review,* Vol. 23, 2020, pp. 216-217, 220 e 223. Sobre o tema, entre nós, *vide* ROCHA, Francisco Chilão, "DSP 2 e RGPD: Uma dicotomia nas suas parecenças. Uma visão portuguesa sobre assunto", *in Revista de Direito Financeiro e dos Mercados de Capitais*, vol. 2, n.º 9, 2020, disponível em https://www.blook.pt/home (02.10.2020), pp. 355-367.

[88] *Vide* THE EUROPEAN DATA PROTECTION BOARD, *EDPB PSD2 Letter*, EDPB-84-2018, Bruxelas, 2018, disponível em https://www.edpb.europa.eu (1.12.2019) e THE EUROPEAN DATA PROTECTION BOARD, *Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR*, 2020, disponível em https://www.edpb.europa.eu (22.05.2021).

[89] *Vide* THE EUROPEAN DATA PROTECTION BOARD, *EDPB PSD2 Letter*..., cit., pp. 3 e 4 e THE EUROPEAN DATA PROTECTION BOARD*, Guidelines 06/2020 on the interplay…,* cit., pp. 14 e 15.

[90] A aceitação generalizada das cláusulas de um contrato já chocaria com as exigências do consentimento nos termos do RGPD, quando estamos perante um tratamento cuja base de licitude seja o consentimento do titular, nos termos da al. a), do n.º 1, do art. 6.º, do RGPD. Como referiu GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS na p. 18 das suas *Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*, WP259 rev. 01, 2018, disponível em https://www.edpb.europa.eu (8.05.2020), "o responsável pelo tratamento também deve ter cuidado com o facto de o consentimento não poder ser obtido através da mesma ação de concordar com o contrato ou aceitar as condições gerais do serviço. A aceitação generalizada de condições gerais não pode ser encarada como ato positivo inequívoco que dá consentimento para a utilização dos dados pessoais". Tal exige-se, por exemplo, para o tratamento de dados não necessários para a execução do contrato ou para as categorias especiais de dados.

dos mesmos dados e para os mesmos fins, contornar-se-ia o espírito da norma presente no art. 6.º do RGPD, que se evidencia perante a necessidade de cautela quando em causa está a execução de um contrato com a simultânea obtenção do consentimento do titular dos dados mas, neste caso, para o tratamento de outros dados não necessários para os fins da relação contratual. O legislador europeu precaveu tal situação, impedindo a subordinação da prestação contratual, isto é, o acesso aos serviços, da complementar prestação do consentimento do titular para o tratamento de outros dados ou para distintos fins. Tal opção prende-se com os requisitos e características exigidas ao consentimento, pelo que, no caso em análise, embora na cumulação de bases de licitude não estaria em causa permitir o tratamento para outros fins, a subordinação do acesso aos serviços de iniciação não deixa de se figurar contraditória com a exigência de um consentimento livre prevista no art. 4.º, 11), do RGPD. É precisamente nesse sentido que estabelece o n.º 4, do art. 7.º, do RGPD[91], ao convocar para a avaliação da presença de uma manifestação de vontade livre, a existência de um contrato ao qual o consentimento possa estar associado[92]. Com efeito, parece-nos que considerar a exigência do RSP como um consentimento para o tratamento dos dados nos termos do RGPD, seria desvirtuar as regras e requisitos que este diploma prevê para a obtenção do consentimento do titular dos dados, acabando por não consistir num fundamento válido.

Cremos também que a questão em volta da existência da manifestação de uma vontade livre seria sempre de se colocar, na medida em que estamos perante uma relação onde, na grande maioria dos casos, os utilizadores são igualmente consumidores a tentar aceder a bens e serviços indispensáveis[93]. Embora não se trate da abertura de contas bancárias propriamente dita, a evolução e crescente adesão ao comércio eletrónico e a necessidade de manter a segurança nas transações realizadas nesta sede, fazem com que o recurso a estes serviços se possa mostrar essencial para muitos utilizadores, que prestariam o seu consentimento como condição de acesso a tais serviços e independentemente da consciência sobre as consequências desse ato, como forma de os aceder[94].

2.3. A partilha de dados associados às contas de pagamentos e o Regulamento Geral sobre a Proteção de Dados

[91] *Vide* A. BARRETO MENEZES CORDEIRO, "O Consentimento do titular...", cit., p. 48, que refere que, o n.º 4, do art. 7.º, do RGPD em articulação com o considerando 43 do RGPD, vem estabelecer uma presunção de que "estando a execução de um contrato subordinada ao tratamento de dados pessoais que não seja necessário para a execução desse mesmo contrato, o consentimento não será válido".
[92] *Vide* Considerando 42 do RGPD que estabelece que "não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado". A vontade livre surge no RGPD associada à ausência de uma influência ou desequilíbrio de posições, embora tais situações dependam sempre de um juízo concreto.
[93] O EDPB considera que o consentimento previsto na DSP2 deverá ser dado livremente, não podendo o utilizador encontrar-se forçado a fazê-lo. *Vide* THE EUROPEAN DATA PROTECTION BOARD, *Guidelines 06/2020 on the interplay…*, cit., p. 15. Porém, não nos podemos esquecer que o art. 94.º, da DSP2, e o art. 136.º, do nosso RSP, são aplicáveis à prestação de serviços de pagamento em geral, excetuando-se a informação sobre contas, pelo que a necessidade de acesso a tais serviços, centrais na sociedade dos nossos dias, poderá diminuir a liberdade de consentir do utilizador.
[94] Veja-se a referência feita por A. BARRETO MENEZES CORDEIRO, "O Consentimento do titular...", cit., pp. 35-36.

Com o reconhecimento de novos serviços, o RSP vem promover um maior controlo pelo utilizador dos dados das suas contas de pagamento e incentivar a circulação dos mesmos. Isto vai de encontro com o objetivo do direito de portabilidade previsto no art. 20.º do RGPD, que visa conceder ao titular dos dados um papel ativo através da capacidade de transferir para um ambiente informático na sua posse ou de um outro responsável pelo tratamento os dados que possuí junto de outro prestador. Isto leva-nos a considerar que a partilha[95] de dados associados a uma conta de pagamento é uma manifestação desse direito de portabilidade dentro de um domínio legislativo concreto[96]. Este direito permite combater a impossibilidade de reutilização dos dados e, por isso, surge como forma de acautelar o consumidor, ao permitir que este se desvincule do prestador de serviço com maior facilidade, por tal já não implicar a perda das informações conservadas junto do mesmo[97].

O considerando 89 da DSP2 reconhece a possibilidade de a prestação de serviços de pagamento implicar o tratamento de dados pessoais e invoca a aplicação do RGPD[98]. Tal circunstância poderá ocorrer, recorda-se, quando se tratar de informações que permitem identificar os utilizadores que sejam pessoas singulares. Apesar disso, o texto do RSP nem sempre estabelece a melhor articulação com a legislação de proteção de dados, como se apontou, bem como pela exclusão dos serviços de informação sobre contas do art. 136.º, relativo à proteção de dados pessoais, por força da exceção prevista no art. 22.º, n.º 2. Não se consegue descortinar a *ratio* de tal exclusão, uma vez que, pela natureza dos serviços de informação sobre contas, a sua atividade é a que traz maiores exigências de regulação e implementação de medidas de segurança no acesso e tratamento de dados[99]. Apesar disso, na prática, não se configura como problemática a exclusão dos referidos serviços pelo RSP do normativo sobre a proteção de dados, uma vez que a legislação sobre a proteção de dados e privacidade será sempre de se aplicar ao tratamento de dados que os PSIC possam realizar no

[95] O EDPB adianta que o tratamento de dados pelo PSPGC que consiste, precisamente, na concessão de acesso aos dados solicitados pelo PSIP para a prestação dos seus serviços tem como fundamento o cumprimento de uma obrigação legal derivante do RSP, consistindo num tratamento lícito por força da alínea c), do n.º 1, do art. 6.º, do RGPD. *Vide* THE EUROPEAN DATA PROTECTION BOARD*, Guidelines 06/2020 on the interplay…,* cit., p. 12.

[96] Reconhecendo que diferentes tipos de portabilidade de dados podem ser previstos noutros domínios legislativos, vide GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações sobre o direito à portabilidade dos dados,* WP242 ver. 01, 2017, disponível em https://www.edpb.europa.eu (21.07.2020), p. 4. Em sentido semelhante, *vide* DIOGO PEREIRA DUARTE e ALEXANDRA GUSEINOV, "O direito de portabilidade de dados pessoais", *in FinTech II: Novos Estudos sobre Tecnologia Financeira*, CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Coord.), Coimbra, Edições Almedina, 2019, pp. 111-112 e 126-127. Neste último caso, os Autores referem que o direito de portabilidade surge, no âmbito da DSP2, essencialmente como um instrumento de potencialização do surgimento de novos operadores.

[97] Sobre como o direito de portabilidade de dados pessoais surge para proteger o consumidor, *vide* DIOGO PEREIRA DUARTE e ALEXANDRA GUSEINOV, "O direito de portabilidade...", cit., pp.109-110, em especial, nota de rodapé 6. Nesta matéria, os Autores fazem referência precisamente ao exemplo do titular de uma conta bancária que evita mudar de prestador de serviços para não perder o seu histórico de transações.

[98] O considerando 89 da DSP2 faz referência à Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 que previa, igualmente, a obtenção de um consentimento livre do titular. Foi posteriormente revogada pelo RGPD. Por isso, devemos proceder a uma interpretação atualista do mesmo e considerar que as regras do RGPD são aplicáveis ao tratamento de dados pessoais para efeitos da DSP2 e do RSP.

[99] A exclusão de aplicação do requisito contratual adicional previsto no art. 136.º à prestação de serviços de informação sobre contas vem enfraquecer a relevância que este poderia possuir no âmbito do reforço da posição do utilizador em matéria de proteção de dados.

âmbito da prestação dos seus serviços, tendo de ser igualmente respeitadas as obrigações que sobre o responsável de tratamento impendem[100].

Por outro lado, a al. f), do n.º 3, do art. 106.º, interdita o PSIP de exigir dados que extravasem o necessário para o contrato de prestação do serviço, consagrando uma manifestação do princípio da minimização dos dados previsto no art. 5.º, n.º 1, al. c), do RGPD. Esse princípio surge intrinsecamente associado ao princípio da limitação de finalidades[101], pelo que o próprio RSP prevê na al. g), do n.º 3, do art. 106.º, a restrição do acesso, utilização e armazenamento dos dados ao concreto serviço solicitado pelo utilizador. Note-se que, a opção por uma diferente consagração da limitação das finalidades do tratamento na disciplina dos novos serviços, não deixa de se mostrar curiosa, dado que, no caso da iniciação de pagamentos, os prestadores devem limitar o tratamento dos dados ao estritamente necessário ao serviço[102] solicitado, ao passo que em relação aos serviços de informação sobre contas é acrescentada a menção de que a mesma limitação é feita "de acordo com as regras em matéria de proteção de dados"[103]. Como referem Wolters e Jacobs, a particular menção sugere que os prestadores de serviços de informação sobre contas podem proceder a um tratamento subsequente para outras finalidades não incompatíveis e em concordância com o que o RGPD permite no art. 6.º, n.º 4, ao contrário do que sucederia com os serviços de iniciação. Diferentemente, o EDPB não parece conferir qualquer significado à diferente formulação prevista nos normativos, considerando que do RSP não conseguimos retirar outra conclusão que não a de que o prestador, no âmbito concreto da prestação dos serviços de iniciação e de informação sobre contas, vê vedada a possibilidade de tratamento para outros fins por imposição do regime legal[104] que norteia a sua atividade e que determina, à partida, qualquer outra finalidade como incompatível[105], entendimento que nos parece o mais adequado. Esta limitação não nos afigura repreensível considerando a natureza da atividade que facilmente invocará a incompatibilidade de tratar os dados para outros fins, na medida em que estes iriam certamente extravasar as finalidades determinadas inicialmente. Apesar disso, não se entende que o preceituado afasta completamente as regras plasmadas no RGPD, como bem reconhece o regime no art. 136.º, n.º 2, bem como a DSP2 no considerando 89. Posto isto, não se configura como suficiente para obstar a um subsequente tratamento com base no consentimento válido do utilizador ou com base em disposições de direito nacional ou da União Europeia. Apesar disso, não nos esqueçamos que a exigência do consentimento do utilizador poderá, em concreto, configurar uma violação dos princípios referidos, bem como não consistir num consentimento válido por tudo o que já se expôs *supra*.

---

[100] *Vide* P.T.J WOLTERS; B.P.F JACOBS, "The Security of access to accounts under the PSD2", *in Computer Law and Security Review,* Vol. 35, n.º 1, Elsevier B.V, 2019, disponível em https://www.sciencedirect.com (29.11.2019), pp. 33-34.

[101] Sobre os princípios relativos ao tratamento de dados, *vide* A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados...*, cit., pp. 152-163.

[102] Tendo em consideração a atividade desenvolvida pelo PSIP, este terá de possuir um acesso seriamente limitado aos dados do utilizador, relevando, essencialmente, o número da conta, a existência de saldo e as credenciais de segurança personalizadas para autenticação, quando a *interface* e o método de autenticação adotado o exigem.

[103] Cfr. art. 107.º, n.º 2, alínea f).

[104] *Vide* P.T.J WOLTERS; B.P.F JACOBS, "The Security of access…", cit., p. 32.

[105] *Vide* THE EUROPEAN DATA PROTECTION BOARD*, Guidelines 06/2020 on the interplay…,* cit., pp. 11 e 12.

No que contende com os géneros de dados que os terceiros prestadores podem ter acesso, a EBA avançou que os terceiros prestadores não poderão aceder a dados que revelem a identidade do utilizador, tais como a morada, a data de nascimento e o número de segurança social[106]. Não é indiscutível aquilo que se pode considerar como dados que revelem a identidade do utilizador, uma vez que quaisquer dados pessoais do mesmo que possam servir para o identificar e diferenciar poderão manifestar a identidade do titular por permitirem essa individualização. Mas o limite imposto pelo RGPD e pelo RSP é claro, os prestadores têm de se cingir sempre àquilo que é estritamente necessário para a prestação do serviço de iniciação de pagamentos.

Outras questões têm sido levantadas em sede de proteção de dados no âmbito dos serviços de pagamento. É o caso do *silent party data processing*[107], expressão utilizada para referir o tratamento de dados de titulares que não possuem uma relação com o prestador de serviços, nem consentiram no acesso aos seus dados pessoais, podendo tal ocorrer mesmo sem que o titular tenha consciência ou conhecimento disso[108]. Será o caso do segundo titular de uma conta conjunta que não solicitou o serviço de iniciação, bem como do próprio beneficiário das transações[109]. Se não estamos perante a execução de um contrato ou a prestação de consentimento pelo contitular ou beneficiário, o acesso a dados que a esse titular possam dizer respeito só poderia ser lícito a coberto de um interesse legitimo do prestador, como permite a al. f), do art. 6.º, do RGPD. O EDPB considerou precisamente que o acesso a dados pode ser considerado lícito ao abrigo de um interesse legítimo[110] do prestador desde que não existam interesses e direitos fundamentais do titular dos dados que se sobreponham[111]. Esta situação, embora nos pareça surgir com maior frequência no contexto dos serviços de informação sobre contas, não deixa de configurar uma hipótese no âmbito da iniciação de pagamentos, na medida em que o número da conta e as credenciais de segurança personalizadas são dados que se referem também ao eventual contitular, embora possam não permitir diferenciar completamente entre os dois titulares da conta[112].

---

[106] EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC* (EBA-OP-2018-04), 2018, disponível em https://www.eba.europa.eu (17.05.2020), p. 6.
[107] Em português, por tradução nossa, "tratamento de dados de parte silenciosa".
[108] THE EUROPEAN CONSUMER ORGANISATION, *BEUC's Recommendations to the EDPB* (…), cit., p. 4.
[109] O tratamento de dados de partes silenciosas assumirá contornos semelhantes ao que acontece com os dados acedidos pelo PSPGC sobre os beneficiários das operações que não sejam igualmente seus clientes. Na prestação dos serviços de iniciação, a hipótese do beneficiário tratar-se de uma parte silenciosa parece-nos menos provável, dado que, o modelo de negócio inerente aos serviços de iniciação requer o conhecimento dos mesmos por parte do beneficiário e uma relação com este. *Vide* P.T.J WOLTERS; B.P.F JACOBS, "The Security of access…", cit., pp. 32-33.
[110] *Vide* THE EUROPEAN DATA PROTECTION BOARD*, Guidelines 06/2020 on the interplay…,* cit., pp. 16 e 17.
[111] O prestador de serviços de pagamento não poderá tratar os dados que possuiu sobre a parte silenciosa para outras finalidades que não as que motivou o conhecimento daqueles dados, exceto com base em legislação europeia ou nacional que o legitime. Ainda neste âmbito, o EDPB considera que não há igualmente fundamento legal para o prestador poder recolher os dados necessários para obter o consentimento da parte silenciosa com vista a um tratamento para outras finalidades. *Vide* THE EUROPEAN DATA PROTECTION BOARD*, Guidelines 06/2020 on the interplay…,* cit., p. 17.
[112] A prestação de serviços de informação sobre contas é suscetível de revelar, de modo mais amplo, dados pessoais que permitem uma melhor identificação do segundo titular da conta de pagamento, nomeadamente, através das operações e transações que realiza e os respetivos beneficiários.

De idêntico modo, as operações de pagamento realizadas por um utilizador poderão revelar dados que se subjazem a categorias especiais[113] previstas no RGPD[114]. De acordo com o postulado no n.º 2, do art. 9.º, do RGPD, para legitimar o tratamento de dados sensíveis não basta que estes sejam necessários à execução de um contrato celebrado com o titular, exige-se razões mais fortes para o tratamento de dados de tais categorias, ou, se nenhuma das hipóteses se verificar, o consentimento explícito do titular. Não nos parece que os serviços de iniciação estejam isentos de se depararem com transações relacionadas com dados sensíveis do titular, mas, surgindo tais serviços no âmbito do comércio eletrónico, o mais provável é que se trate, na maioria, de transações de consumo comum e que poucas informações de natureza sensível revelem sobre a pessoa do utilizador. A não ser assim, não será permitido aos terceiros prestadores aceder e utilizar dados sensíveis sem o preenchimento de alguma exceção prevista no art. 9.º, n.º 2, do RGPD, pelo que caberá a esses prestadores diligenciar no sentido de garantir que há legitimidade para o tratamento, sob pena de se considerar o tratamento ilícito. Por sua vez, ambos os prestadores envolvidos terão de diligenciar no sentido de aplicar medidas técnicas que impeçam o acesso a dados sensíveis do utilizador que não são necessários e/ou não seja lícito o seu conhecimento[115]. Competirá ao terceiro prestador garantir, na necessidade de tratar dados sensíveis, que se encontre preenchida alguma derrogação da proibição de tratar tais dados, como será o caso em que o titular consente explicitamente e devidamente a um conjunto discriminado de dados, independentemente do modelo de negócio e *interface* que utilize para prestar os seus serviços.

Assim, no que concerne à proteção dos dados pessoais dos utilizadores, compete às entidades intervenientes pautarem-se pela adoção de medidas técnicas e organizativas que garantem a segurança adequada aos riscos que a prestação dos seus serviços envolve, por força do disposto no artigo 32.º do RGPD. É certo que este novo panorama de abertura traz pesados desafios e responsabilidades às instituições tradicionais, sobre quem impende a obrigação de desenvolver *interfaces* adequadas para o acesso dos terceiros prestadores, mas também de garantir todos os outros mecanismos necessários à proteção da conta e dos dados do titular. Apesar disso, tal não pode resultar na desoneração dos terceiros prestadores de adotarem, igualmente, medidas de segurança que assegurem o tratamento de dados em segurança, uma vez que as regras que vinculam os bancos enquanto responsáveis pelo tratamento têm, do mesmo modo, os terceiros prestadores como destinatários.

[113] O RGPD define, no art. 9.º, n.º 1, como dados sensíveis todas as informações que "revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa".

[114] A BEUC refere como exemplo de transações que possam revelar dados sensíveis do titular, aquelas que registem pagamentos ou doações para um partido político ou para uma organização religiosa, o pagamento de mensalidade referente à subscrição de uma revista religiosa, de taxas relativas à filiação de um grupo sindical ou pagamentos alusivos a tratamentos médicos. *Vide* THE EUROPEAN CONSUMER ORGANISATION, *BEUC's Recommendations to the EDPB* (…), cit., pp. 4-5.

[115] Sobre o tratamento de categorias especiais de dados pelos prestadores de serviços de pagamentos, *vide* THE EUROPEAN DATA PROTECTION BOARD, *Guidelines 06/2020 on the interplay…,* cit., pp. 18 a 21.

3. A segurança no acesso às contas e na execução das operações de pagamento

A revisão da legislação dos serviços de pagamento pautou-se pela preocupação da inclusão de requisitos legais que melhorassem as medidas de segurança adotadas pelos prestadores de serviço e reforçassem a autenticação do utilizador, uma vez que a versão anterior demonstrou-se insuficiente perante o surgimento de mecanismos de fraude cada vez mais sofisticados e impercetíveis por parte do utilizador, à medida que as operações de pagamento se realizavam, cada vez mais, através da Internet, onde se registou a maioria das perdas decorrentes de operações fraudulentas[116]. Perante o reporte de um nível muito elevado de fraude nas operações *online* e a evidência da necessidade de um profundo reforço de segurança na execução dos pagamentos, as entidades europeias tomaram iniciativas com vista a efetivar a proteção dos utilizadores nas operações realizadas através da Internet, nomeadamente, com a publicação pela EBA, em dezembro de 2014, das Orientações sobre a segurança dos pagamentos efetuados através da Internet, surgindo como a primeira fase do processo do incremento da segurança dos pagamentos pela Internet, prevendo-se a conclusão do mesmo com a adoção de requisitos mais rigorosos pela DSP2[117]. Já nas suas orientações, a EBA previa a implementação, por parte dos prestadores de serviço, de uma autenticação forte dos utilizadores em moldes idênticos aos previstos atualmente no RSP[118].

A par da necessidade de regular os contornos da autenticação forte do utilizador nas operações que exigem a mitigação do risco de fraude, uma das preocupações primordiais da abertura dos sistemas dos bancos a outros prestadores de serviços contende com a partilha das credenciais de segurança personalizadas por parte do utilizador, incindindo não só um risco elevado no ato de dar a conhecer a um terceiro as suas credenciais, como também no processo que subjaz tal comunicação. É nesta sede que são de aplicar as normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras previstas no Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de novembro de 2017 (NTR/NAC)[119].

---

[116] Em relação à utilização de cartões, instrumento que assume um papel central na vida dos consumidores, segundo o último relatório do Banco Central Europeu sobre a fraude na utilização de cartões, a fraude registada em operações de *card-not-present*, isto é, através da Internet, representa 79% do total de operações fraudulentas registadas no ano 2018, um aumento de 17.71% em relação a 2017, o que equivale a perdas no valor de 1.43 mil milhões de euros. No global, o aumento das operações fraudulentas com cartões situa-se nos 13% em comparação ao ano de 2017, registando um total de perdas no valor de 1.80 mil milhões de euros. A fraude nas operações realizadas à distância são as que mantêm um crescimento constante nos últimos anos, ao contrário da utilização do cartão em pontos físicos como é o caso da sua utilização em pontos ATM. Há 5 anos, no ano da publicação da DSP2, as operações fraudulentas sem cartão presente representavam 71% do total das operações. *Vide* EUROPEAN CENTRAL BANK, "Sixth Report on Card Fraud", 2020, disponível em https://www.ecb.europa.eu (24.08.2020).

[117] AUTORIDADE BANCÁRIA EUROPEIA, *Orientações sobre a segurança dos pagamentos efetuados através da internet* (EBA/GL/2014/12_Rev1), 2014, disponível em https://www.eba.europa.eu (20.08.2020). Sobre as iniciativas em matéria de segurança, *vide* MARY DONNELLY, "Payments in the Digital Market: Evaluating the contribution of Payment Services Directive II", *in Computer Law and Security Review*, vol. 32, n.º 6, Elsevier Ltd., 2016, disponível em https://www.sciencedirect.com (29.11.2019), p. 836.

[118] *Vide* AUTORIDADE BANCÁRIA EUROPEIA, *Orientações sobre a segurança*..., cit., pp. 6, 13 e 14.

[119] Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de novembro de 2017, que complementa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras, *in JO L 69 de 13.3.2018*.

3.1. A autenticação forte do utilizador

Uma das alterações fundamentais do RSP prende-se com a harmonização e reforço dos requisitos de segurança aplicáveis às operações de pagamento em todos os Estados-Membros. De acordo com a al. c), do art. 2.º, deverá entender-se por autenticação o procedimento que permite ao prestador verificar a identidade de um utilizador ou a validade da utilização de um instrumento, incluindo o próprio uso das credenciais de segurança personalizadas do utilizador, pelo que a exigência de uma autenticação forte do cliente impõe que o referido procedimento de verificação se baseie na utilização de "dois ou mais elementos pertences às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é)". Em relação ao primeiro elemento, na recente opinião da EBA sobre os elementos que integram a autenticação forte do cliente[120], faz-se referência de que poderá consistir numa palavra-passe, um código ou respostas baseadas em conhecimento que só o utilizador poderá ter, mas que já não preencherá o conceito o valor de verificação do cartão (CVV) e a sua data de validade, bem como a sua identificação de utilizador[121]. No que toca ao elemento posse, a EBA considera que poderá estar em causa o telemóvel do utilizador ou um dispositivo de autenticação, sendo que a posse deverá ser confirmada através da criação ou receção de um elemento de validação dinâmica no dispositivo como o envio de uma senha ou código único. Já não será suficiente a posse de um cartão matriz comprovada com a introdução dos dados do cartão[122]. Por fim, o elemento inerência que, certamente, melhor garante a correta verificação do utilizador, basear-se-á, essencialmente, em características físicas e comportamentais do utilizador, ou seja, dados biométricos, como é o caso do reconhecimento facial, de voz e da impressão digital[123]. A utilização dos referidos elementos tem de ser independente de modo a que a violação de um deles não comprometa a fiabilidade dos outros e a autenticação deverá ser realizada sempre de forma a proteger a confidencialidade dos dados de autenticação. Embora nada na letra da lei o impeça, pela sua razão de ser e de modo a cumprir o seu objetivo, os elementos utilizados na autenticação do utilizador têm de ser de natureza diferente[124].

---

[120] EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2,* EBA-Op-2019-06, disponível em https://www.eba.europa.eu (4.10.2019).
[121] *Vide* EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on the implementation of the RTS*…, cit., p. 7.
[122] *Vide* EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on the elements*…, cit., pp. 6-7.
[123] A utilização de dados biométricos para a autenticação do utilizador envolve várias questões pertinentes, como a recolha e tratamento desses dados, bem como o consentimento específico para o mesmo, à luz da legislação da proteção de dados vigente. Pela limitação do nosso estudo, não se poderá aprofundar a relevância da questão mas importa salientar que a EBA já teve oportunidade de estatuir que quando a autenticação do utilizador se dê com um elemento baseado em dados biométricos, tal elemento nunca poderá ser transmitido ao PSIP para poder aplicar o procedimento de autenticação disponibilizado pelo PSPGC. Apesar disso, a autenticação não poderá deixar de se proceder da mesma forma pelo que o PSPGC vê-se obrigado a aplicar o redireccionamento da autenticação, *vide* EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC,* EBA/OP/2020/10, 2020, disponível em https://www.eba.europa.eu (22.08.2020), p. 4. Esta mostra-se como a solução que melhor tutela a privacidade do utilizador.
[124] Nesse sentido, *vide* EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on the implementation of the RTS* (…), cit., p. 7.

Antes da iniciação da operação[125], o PSIP é obrigado a aplicar a autenticação forte do utilizador que não se basta apenas com a combinação de dois dos elementos referidos *supra*, exigindo-se, por remissão do n.º 4, do art. 104.º, para o n.º 2 do mesmo preceito, que na autenticação se inclua uma ligação dinâmica que associe a operação ao montante a transferir e ao específico beneficiário, por se tratar de operações de pagamento eletrónico remotas[126]. Exige-se, assim, uma autenticação "qualificada" ou "dinâmica"[127], que pressupõe a geração de um código que deverá ser único para cada momento de autenticação[128].

O RSP reconhece o direito ao PSIP de se basear nos procedimentos de autenticação forte e dinâmica facultados pelo PSPGC ao utilizador[129]. O diploma não densifica, nem o faz as NTR/NAC, em que moldes tal possibilidade pode ocorrer, pelo que ficará dependente da *interface* adotada pelo PSPGC. A utilização do procedimento de autenticação do banco pelo PSIP não parece surgir na lei como uma única via, obrigatória por força da imposição da necessidade de uma autenticação dinâmica na iniciação da operação por parte do PSIP, mas antes como uma possibilidade, sugerindo que o PSIP pudesse desenvolver e adotar o seu próprio procedimento de autenticação forte do utilizador, desde que de acordo com os requisitos da lei[130]. Como bem alertam Wolters e Jacobs, a utilização de um procedimento alternativo de autenticação poderá trazer riscos adicionais, tanto pela adição de outra fase à iniciação e execução das operações de pagamento que, por isso, pode ser intercetada e acedida por terceiros não autorizados com o objetivo de proceder a ações fraudulentas na conta, bem como pela dificuldade de identificação do utilizador perante o PSPGC, uma vez que este só poderá confirmar que o ordenante é o titular da conta de pagamento mediante os procedimentos por si adotados e da utilização das credenciais de segurança que cede ao utilizador para o efeito. Entendem os Autores que a melhor forma de mitigar os riscos associados a esta possibilidade passa pela exigência de um acesso autorizado com o procedimento de autenticação do PSPGC de modo a legitimar os posteriores acessos que se dão apenas com a autenticação do PSIP. Por sua vez, a lei não prevê que o PSPGC pudesse impor essa necessidade de autenticação única ou anual. Porém, tal poderia derivar da obrigação que impende sobre o prestador de prevenir qualquer acesso não autorizado por

[125] Dado que o PSIP realiza duas ações que exigem a aplicação de autenticação forte, isto é, o acesso à conta em linha e a iniciação de uma operação de pagamento eletrónico remota, o procedimento de autenticação seria de se aplicar em cada uma destes momentos. A EBA pronunciou-se pela desnecessidade de aplicação de dois procedimentos de modo a reduzir os obstáculos na prestação de serviços de iniciação e a manter a facilidade de uso pelo utilizador, salvo se o PSPGC considere que existem razões de segurança para tal, que se deverão prender com a suspeita de fraude em relação a uma operação em particular, devendo ser capaz de provar essa circunstância perante o Banco de Portugal. Optou, por sua vez, por considerar de modo diverso para os casos em que o PSIP não comunica, desde logo, que conta de pagamento do utilizador pretende aceder, pelo que deverá ser de aplicar a autenticação para a seleção da conta a debitar e, posteriormente, a iniciar o pagamento. *Vide* EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on obstacles…*, cit., p. 6.

[126] As operações de pagamento eletrónico remotas, são, de acordo com a al. *kk*), do art. 2.º, todas as operações iniciadas através da Internet.

[127] A classificação da autenticação prevista no n.º 2 do art. 104.º como uma autenticação "qualificada" e "dinâmica" é avançada por MARIA RAQUEL GUIMARÃES, em "O comércio electrónico ‹‹está na moda››?..., cit., p. 852 e "Pagamentos electrónicos...", cit, n.os 2 e 3.

[128] *Vide* considerando 95 da DSP2.

[129] V. art. 104.º, n.º 6.

[130] Explorando a possibilidade do PSIP desenvolver o seu próprio procedimento de autenticação do utilizador, *vide* P.T.J WOLTERS; B.P.F JACOBS, "The Security of access…", cit., pp. 38-39.

força do dever de gestão dos riscos operacionais e de segurança previsto no art. 70.º, n.º 1, ao qual o PSIP também está vinculado.

Apesar do exposto, parece-nos pertinente questionar, mais do que a possibilidade do PSIP aplicar um procedimento de autenticação próprio, se aos PSPGC é permitido isentar o seu procedimento de autenticação em detrimento da utilização, por parte do titular da conta, dos meios de autenticação facultados pelo PSIP. Em moldes semelhantes à obrigação que recai sobre o PSIP, o PSPGC encontra-se obrigado a aplicar autenticação forte e dinâmica nas operações de pagamento eletrónico remotas, pelo que o mero recurso pelo utilizador a um serviço de iniciação não pode significar, sem mais, que o PSPGC fica isento de tal obrigação, quando, mais do que nunca, deverão ser implementadas medidas que garantem a segurança no processo transacional.

Note-se também que, se o PSPGC do ordenante não aplicar a autenticação dinâmica exigida, não poderá exigir, no caso de operações não autorizadas, que o utilizador suporte as perdas resultantes das mesmas, nem mesmo dentro do limite legal previsto, pelo que caberá ao PSPGC suportar todas as perdas que derivam da operação não autorizada. Isto diz-nos que não se poderá confiar ao PSIP a decisão sobre tal opção, quando em causa está uma responsabilidade que poderá vir a ser imputada ao PSPGC, pelo que a previsão do RSP só fará sentido se a decisão de aplicar a autenticação forte do utilizador estiver na disponibilidade do prestador de serviços que lhe gere a conta, não subordinando a utilização dos seus próprios procedimentos à não adoção de outros mecanismos por parte dos terceiros prestadores. Posto isto, se o PSPGC quiser afastar a responsabilidade prevista no n.º 5, do art. 115.º, tem de aplicar os seus procedimentos de autenticação forte e dinâmica. Na mesma linha, a isenção da obrigação de aplicação da autenticação forte só poderá dar-se nas exceções previstas nas NTR/NAC, que estão estipuladas de modo a serem aplicadas por quem gere a conta do utilizador[131].

A consideração de que o PSPGC terá de aplicar os seus procedimentos de autenticação mesmo em operações iniciadas por um PSIP[132], é confirmada pela EBA na sua opinião sobre a implementação das NTR/NAC, ao afirmar que apenas o PSPGC poderá aplicar a autenticação forte do utilizador em relação à sua conta de pagamento, bem como é ao mesmo que compete aplicar as exceções à aplicação da mesma[133]. A análise de risco das operações, para uma

[131] O capítulo III das NTR/NAC prevê um elenco de várias isenções da autenticação forte do utilizador relacionadas, na sua maioria, com o acesso a informações sobre o saldo da conta e operações realizadas, com o baixo valor das transações, a certificação de beneficiários, operações recorrentes no mesmo montante e a favor do mesmo beneficiário, como na utilização do instrumento de pagamento em pontos físicos. A exceção que se poderá configurar mais ampla, mesmo no caso de pagamento eletrónico remoto, é a prevista no art. 18.º do diploma, que só será de se aplicar quando apresentam um baixo nível de fraude.

[132] Embora de forma não densificada, mas assumindo que a autenticação se dá com base nos procedimentos facultados pelo PSPGC, *vide* FRANCISCO MENDES CORREIA, "DSP 2 e Normas Abertas...", cit., p. 164. De modo semelhante e considerando que os terceiros prestadores podem autenticar-se em representação do utilizador, *vide* GIOVANNI BERTI DE MARINIS, "La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2" *in Riviste Diritto della banca e del mercato finanziario*, 4/2018, Pisa, Pacini Editore SRL, 2018, p. 648.

[133] *Vide* EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on the implementation of the RTS*..., cit., p. 8. Apesar de considerar que cabe ao PSPGC aplicar a autenticação forte e dinâmica do utilizador relativa à conta que gere, a EBA considerou a hipótese de o PSPGC delegar o procedimento de autenticação a terceiros prestadores para que o façam em substituição e em nome do PSPGC. Porém, tal hipótese não pode ser

eventual isenção da autenticação, também deverá ser efetuada pelo PSPGC. De outro modo não faria sentido, uma vez que é ao mesmo que cabe gerir a conta do utilizador e garantir que a mesma só é acedida por pessoas autorizadas pelo utilizador, pelo que só pela autenticação do mesmo poderá o PSPGC associar o pedido de acesso e da ordem de pagamento ao legítimo titular da conta.

Posto isto, e como reconheceu a EBA, o PSIP poderá querer adotar o seu próprio procedimento de autenticação na sua plataforma, que maior razão de ser ganha quando entre o PSIP e os utilizadores do seu serviço se estabelece uma relação duradoura mediante a celebração de um contrato-quadro, surgindo, neste caso, como um reforço da segurança e proteção do utilizador. Mas tal não poderá resultar na isenção de aplicação da autenticação forte pelo PSPGC em relação à conta de pagamento. Assim, só a obrigação da aplicação dos procedimentos de autenticação forte do prestador de serviços que gere a conta de pagamento cumprirá o acesso seguro à conta e aos dados do utilizador e é o que melhor previne acessos fraudulentos e operações não autorizadas[134]. Isto sem colocar em causa a capacidade técnica do PSIP de adotar mecanismos suficientemente protetores da conta do utilizador, mas que nunca se mostrariam suficientes para o PSPGC reconhecer a legitimidade do ordenante em relação a uma determinada conta de pagamento.

3.2. A *interface* de acesso às contas de pagamento por parte do PSIP

A prestação de serviços de iniciação por parte de outro prestador está dependente da conduta adotada pelo PSPGC, pelo que, quando este disponibiliza a conta de pagamento *online* para o utilizador, é obrigado a desenvolver *interface*s que assegurem a interoperabilidade com o *software* do PSIP e que lhe permita iniciar de forma segura uma ordem de pagamento e receber todas as informações sobre a iniciação e execução da operação[135]. Para que aconteça, o PSPGC tem que optar pela criação de uma *interface* dedicada para o acesso específico de terceiros prestadores ou adaptar a *interface* disponibilizada ao utilizador. Qualquer uma das opções terá de permitir a identificação do PSIP enquanto tal, que se deverá basear em certificados qualificados de selos eletrónicos ou certificados qualificados de autenticação de sítios *Web*, nos termos da legislação europeia relativa à identificação eletrónica e aos serviços de confiança para as transações eletrónicas, pelo que a *interface* terá de ter capacidade para suportar tais certificados[136].

imposta ao PSPGC pelo PSIP, compete ao primeiro decidir pela delegação dessa competência. *Vide* EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on obstacles…*, cit., p. 7.

[134] A não aplicação da autenticação forte do PSPGC poderia resultar no acesso de partes não autorizadas pelo titular da conta, bem como, resultar na não coincidência entre o ordenante e o titular da conta. Tal hipótese coloca em causa o reforço de segurança que o RSP quis implementar.

[135] *Vide* art. 30.º, n.º 1, al. a) e c), das NTR/NAC.

[136] O art. 34.º, n.º 1, das NTR/NAC, remete a matéria para o Regulamento (UE) n. ° 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

Os bancos vêem-se onerados com a pesada competência de assegurar que as infraestruturas desenvolvidas permitem que o PSIP cumpre todas as obrigações a que está adstrito por força do RSP. A *interface*[137] dedicada, ou adaptada, tem de assegurar a manutenção de sessões de comunicação entre o PSPGC, o PSIP e o utilizador durante todo o processo de autenticação e iniciação[138], pelo que, inerentemente ligado à opção de *interface* adotada pelo PSPGC, está o procedimento de autenticação do utilizador, que se pode dar mediante diferentes métodos, designadamente, por redireccionamento para a página de *homebanking* disponibilizada ao utilizador, por uma abordagem desacoplada que pressupõe que a autenticação se dê de forma separada do restante processo através de outro dispositivo ou aplicação especifica para o efeito ou, mediante um método incorporado, que já consistirá em fornecer ao PSIP as credenciais de segurança personalizadas cedidas pelo PSPGC numa página que o PSIP lhe apresente para o efeito[139]. O RSP não fixou nenhum método preferencial, cedendo liberdade de atuação ao PSPGC desde que a escolha assegure a segurança nas sessões de comunicação e que as credenciais e códigos de autenticação sejam transmitidos de forma encriptada, a fim de garantir a confidencialidade e integridade dos mesmos[140].

A necessidade de uma *interface* de acesso surge, precisamente, para contornar a utilização por parte dos terceiros prestadores da mesma *interface* que o utilizador[141], que lhes permitia aceder ilimitadamente a todos os dados disponíveis na conta de pagamento *online*, podendo extraí-los nos mesmos modos em que se apresentam, uma vez que acediam à conta como se do utilizador se tratasse[142]. Acresce que, tal pressupunha que o utilizador transmitisse as suas credenciais de segurança ao terceiro prestador. Esta opção mostra-se incompatível com a disponibilidade limitada dos dados ao PSIP que já se referiu, bem como com a garantia de que o acesso à *interface* seja o mais breve possível, cessando logo que a operação tenha sido iniciada[143].

De modo relativamente semelhante, a opção por uma abordagem incorporada de autenticação mediante a *interface* exige que o PSIP tenha acesso às referidas credenciais do utilizador e seja o mesmo PSIP a autenticar-se junto do PSPGC, com vista a iniciar o pagamento. Esta opção é a que maior hesitação invoca quando vista em confronto com a necessidade de se

---

[137] Em Portugal, foi desenvolvido pela Sociedade Interbancária de Serviços (SIBS) em conjunto com vários bancos, como é o caso da Caixa Geral de Depósitos, a SIBS API Market, uma *interface* desenvolvida especialmente para o acesso de terceiros prestadores de serviços de pagamento. A iniciativa conjunta visa padronizar as regras e procedimentos de acesso, o que permitirá melhor adaptar o *software* e sistemas de todos os intervenientes. V. https://www.sibsapimarket.com/payments-2 (23.08.2020).

[138] V. art. 30.º, n.º 2, al. b), das NTR/NAC.

[139] Sobre o reconhecimento de três diferentes métodos de autenticação e da hipótese da combinação dos mesmos, *vide* EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on the implementation of the RTS…*, cit., pp. 10-11.

[140] V. art. 35º, n.º 1, das NTR/NAC.

[141] Apesar das preocupações da EBA no acesso pelos terceiros prestadores pela mesma *interface* – não adaptada – do utilizador, a mesma não deixa de estar presente no mecanismo de contingência previsto no art. 33.º, n.º 4, das NTR/NAC, aplicável quando a *interface* dedicada se encontre com problemas de disponibilidade e desempenho técnico e o PSPGC não beneficia da isenção da obrigação de permitir o acesso alternativo pela mesma *interface* do utilizador, nos termos do n.º 6 do mesmo artigo. Reconheceu também que, quando o PSPGC não possuiu capacidade técnica para confirmar ao PSIP, em tempo real, a existência de fundos suficientes para a transação a iniciar e para que o último possa calcular o risco de confirmar a operação ao beneficiário, que deverá ser permitido aceder aos dados por si mesmo para proceder à avaliação da suficiência de fundos, em alternativa à confirmação prevista no art. 36.º, n.º 1, al. c), das NTR/NAC.

[142] *Vide supra* 1.2.

[143] V. art. 35.º, n.º 2, das NTR/NAC.

tutelar a posição do utilizador em relação ao acesso dos seus dados de pagamento sensíveis, mas que não é afastada pelas NTR/NAC[144]. Diferentemente, o redireccionamento ou uma abordagem desacoplada, permite que o PSIP, em momento algum, tenham acesso às credenciais utilizadas para a autenticação do utilizador, solução que melhor vai ao encontro da proibição do mesmo armazenar esses dados e evita, igualmente, o abuso por parte do PSIP. A utilização de um método incorporado adiciona, sem sombra de dúvidas, um risco acrescido, na medida em que abre porta ao desenvolvimento de novas práticas fraudulentas que tenham como alvo intercetar o momento de transmissão das credenciais pelo utilizador ao PSIP[145]. Reconhece-se que a soma de um novo interveniente no processo de execução das operações acarreta, por si só, um risco adicional, pelo que o esforço desenvolvido por parte das NTR/NAC visa mitigar esta circunstância, nomeadamente, pela exigência de encriptação dos dados transmitidos nas sessões de comunicação, como pela oneração do PSIP em manter as credencias inelegíveis por parte de qualquer membro do seu pessoal e em reportar a quebra de confidencialidade das mesmas ao utilizador e ao PSPGC. De igual modo, o art. 22.º, n.º 2, das NTR/NAC impõe que se garante a dissimulação das credenciais quando as mesmas são visualizadas e que não sejam totalmente legíveis quando o utilizador começa a introduzi-las, de modo a que, em momento algum, seja visível todo o conteúdo das mesmas.

Embora nos pareça que a solução de uma *interface* dedicada que aplique um método desacoplado ou o redireccionamento para a autenticação seja a que melhor protege a integridade da conta de pagamento do utilizador[146], a adoção de tal mecanismo tem de ser feita com cautela, de modo a não colocar obstáculos ao acesso do PSIP e incumprir o disposto no n.º 3, do art. 32.º, das NTR/NAC. Esta norma consagra um regime bastante protecionista do acesso do PSIP, uma vez que afasta a possibilidade do PSPGC impor várias condicionantes a esse acesso e de restringir, ao máximo, a disponibilidade da *interface* e da conta de pagamento em relação ao PSIP. Foi com base nessa norma que vários agentes do mercado, após a entrada em vigor das NTR/NAC, teceram reclamações junto da EBA e das autoridades nacionais competentes em relação às opções aplicadas de *interface* dedicada com redireccionamento por parte dos PSPGC. Apesar da contestação, a EBA confirmou a possibilidade de aplicação de tais métodos, reiterando que as limitações do referido artigo não configuram proibições, mas meros exemplos que quando aplicados de forma desmedida, poderão ser considerados um obstáculo. Observar o disposto nas NTR/NAC como uma imperativa proibição seria limitar a discricionariedade do PSPGC de implementar os mecanismos e procedimentos que melhor possam vir a proteger a integridade das credenciais

[144] Recomendando a não utilização de método incorporado, *vide* THE EUROPEAN CONSUMER ORGANISATION, *Consumer-Friendly Open Banking: Access to Consumer's Financial Data by Third Parties*, *BEUC-X-2018-082*, Bruxelas, 2018, disponível em https://www.beuc.eu (23.11.2019), pp. 5-6. A levantar preocupações semelhantes, *vide* P.T.J WOLTERS, B.P.F JACOBS, "The Security of access…", cit., pp. 36-37.

[145] No momento da transmissão das credenciais pelo utilizador ao PSIP poderão dar-se práticas fraudulentas em moldes semelhantes ao que já sucedeu na autenticação pelo utilizador na sua página de *homebanking*, através da clonagem perfeita dessa página com o objetivo de se apropriar dos dados fornecidos pelo utilizador que o faz com o intento de aceder à sua conta. Não se exclui a possibilidade de se vir a reportar situações em que a *interface* onde o utilizador deverá facultar as suas credenciais de segurança para transmitir ao PSIP sofra com semelhante prática fraudulenta ou seja alvo de um *software* malicioso.

[146] Sobre os benefícios deste método, *vide* P.T.J WOLTERS, B.P.F JACOBS, "The Security of access…", cit., pp. 36-37.

e da conta de pagamento. Por outro lado, parece-nos também que a própria posição do PSIP melhor se acautela numa opção desacoplada ou de redireccionamento da autenticação, na medida em que conseguirá com maior facilidade afastar a sua responsabilidade em relação a uma potencial apropriação indevida dos elementos de autenticação por deficiência do seu sistema.

Posto isto, só será de se considerar como obstáculos as formalidades e requisitos que tornem a emissão da ordem de pagamento através do PSIP mais onerosa e complexa que a realizada diretamente pelo utilizador junto do seu banco, sem que para isso existam exigências técnicas e que permitam a melhor comunicação entre os intervenientes. Caso contrário, admite-se a aplicação de condições adicionais, desde que processadas em tempo breve e que não originem fricções desnecessárias na experiência do utilizador[147].

3.3. A repartição da responsabilidade pelas operações não autorizadas entre o PSIP, o PSPGC e o utilizador dos serviços

A disciplina da responsabilidade pelas operações não autorizadas[148] mereceu particular atenção pelo novo regime, apresentando um conjunto de normativos, embora estruturalmente semelhantes ao anterior, surgem-nos mais densificados, esclarecendo algumas dúvidas de aplicação, mas, por outro lado, introduzindo novas incertezas quanto ao seu conteúdo. Inegavelmente, a inclusão da autenticação forte e dinâmica do utilizador e o reconhecimento da atividade do PSIP trazem alterações que, à medida que os tribunais forem chamados a julgar sobre a matéria, se irão mostrar bastante significativas[149].

Nesta matéria é importante ter em consideração os deveres acessórios de conduta[150] que sobre o utilizador recaem, por decorrência do art. 110.º. Assim, o utilizador está vinculado a um

[147] *Vide* EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on obstacles…*, cit., pp. 2-4 e 10.

[148] Conservou-se o mesmo sentido de operação não autorizada, que será aquela que não seja precedida pelo consentimento do utilizador, legitimo titular da conta ou do instrumento de pagamento, prestado nos termos art. 103.º. Para uma análise mais detalhada sobre o conceito, *vide* REINHARD STEENNOT, "Reduced payer's liability for unauthorized payment transactions under the second Payment Services Directive (PSD2)", *in Computer Law and Security Review,* Vol. 34, Elsevier Ltd., 2018, disponível em https://www.sciencedirect.com (25.08.2020), pp. 955-956.

[149] A maioria das operações não autorizadas deu-se em situações em que não se exigia autenticação forte ou dinâmica do utilizador. Ainda assim, como aponta MARIA RAQUEL GUIMARÃES em "Pagamentos electrónicos...", cit, n.º 1 e em "The transposition of PSD2: Decree-Law 91/2018 of 12 November, the Portuguese experience and what may (or may not) change", *in L'attuazione della seconda direttiva sui servizi di pagamento e "open banking"*, a cura di E. Bani, A. Sciarrone Alibrandi, V. de Stasio, Bergamo, Bergamo University Press/Sestante Edizioni, 2021, n.º 4.1., passou-se a verificar a apropriação, mediante a instalação de *software* malicioso, dos dispositivos móveis utilizados para a autenticação dinâmica do utilizador, com vista à realização de operações fraudulentas. Situação do género foi apreciada pelo Tribunal da Relação do Porto no acórdão de 7 de outubro de 2014, que concluiu pela não existência de censurabilidade do utilizador que forneceu a marca e modelo do seu telemóvel na página que julgava ser do seu banco, tendo depois realizado um *download* solicitado por uma mensagem de texto por considerar não lhe poder ser exigível a elevada experiência e conhecimento que teria sido capaz de detetar a atuação fraudulenta de terceiro.

[150] Sobre a natureza das obrigações do utilizador, em relação aos instrumentos de pagamento, como deveres laterais ou acessórios de conduta que emergem da relação obrigacional complexa estabelecida entre o utilizador e o prestador, *vide* MARIA RAQUEL GUIMARÃES, *O Contrato-Quadro*, cit., pp. 299-320. Também, PATRÍCIA GUERRA, "A realização de operações de pagamento não autorizadas...", cit., pp. 18-21.

dever de zelo e cuidado para com o instrumento de pagamento, devendo, em particular, tomar todas as medidas razoáveis para preservar a segurança das suas credenciais de segurança personalizadas[151]. A par disso, sobre o mesmo recai o dever de comunicar ao PSPGC, "logo que tenha conhecimento dos factos e sem atraso injustificado", a perda, o furto, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento. A presença desses deveres é importante para aferir se a operação, embora não autorizada pelo utilizador, é-lhe imputável por os ter incumprido de forma negligente ou intencional. Não é difícil compreender que, antes da vigência do novo regime, seria possível associar à conduta do utilizador um carácter censurável quando este partilhasse as suas credenciais de segurança a uma terceira entidade, desvinculada do PSPGC, para que esta acedesse à sua conta e prestasse os serviços hoje reconhecidos pelo RSP[152]. Embora o acesso pelo PSIP colida, à primeira vista, com a obrigação do utilizador de zelar pela segurança das suas credenciais, esta circunstância não poderá, à luz das novas regras, ser considerada uma quebra deliberada, levemente ou grosseiramente negligente, para efeitos de responsabilidade do utilizador, uma vez que estamos perante uma exceção legalmente prevista.

Em traços gerais, a estrutura da responsabilidade pelas operações não autorizadas permaneceu intacta. Por um lado, em caso de negligência leve do utilizador, este pode suportar prejuízos até ao limite de 50 euros nos casos de perda, furto, roubo ou apropriação abusiva do instrumento de pagamento[153]. Se ao utilizador for imputado o incumprimento do seu dever

[151] Cfr. art. 110.º, n.º 1, al. a) e n.º 2.

[152] A considerar que a permissão do acesso à conta por terceiros prestadores configurava uma conduta negligente por violação da confidencialidade dos dispositivos de segurança, na altura, à luz da DSP, *vide* JOSÉ MANUEL FARIA, "Acesso a contas bancárias por terceiros no âmbito de operações de pagamento", *in Revista da Banca*, n.º 71, Lisboa, Associação Portuguesa de Bancos, 2011, pp. 34-35. Nesta matéria, os nossos tribunais tiveram oportunidade de se pronunciar em sentido diferente sobre a partilha das credenciais de segurança a terceiros autorizados ou considerados "auxiliares" do utilizador. O Supremo Tribunal de Justiça, no acórdão de 14 de dezembro de 2016, considerou que o acesso por parte da contabilista do utilizador não configurava uma quebra do dever de proteção que recai sobre o mesmo por ser conforme com "a diligência de um homem médio e, por isso, razoável". Em sentido semelhante decidiu o Tribunal da Relação de Coimbra, no acórdão de 2 de fevereiro de 2016, sobre a divulgação dos mesmos dados a sócios e funcionários de uma pessoa coletiva, na medida em que as credenciais permaneceram na esfera de atuação das pessoas ligadas à organização da mesma.

[153] Em relação ao novo limite de 50 euros imposto pelo RSP, surge a questão de saber se esta imputação dá-se perante um caso de negligência leve do utilizador ou se se refere a uma distribuição objetiva das perdas, uma vez que não consagra, à semelhança do que previa o anterior regime, a necessidade de ter havido quebra da confidencialidade dos dispositivos de segurança por parte do utilizador. Pela formulação do início do art. 115.º, n.º 1, atenta-se desde logo à possibilidade do utilizador vir a ser obrigado a arrecadar com perdas até ao montante máximo de 50 euros, salvo se o seu saldo for inferior, e não de que o mesmo é responsável até aquele limite. Isto sugere-nos que há lugar para uma ponderação das circunstâncias subjacentes a todo o processo em que decorreu a operação não autorizada, o que não deixa de nos remeter para que, nesta possível ponderação, seja de se incluir a existência ou inexistência de uma negligência leve para decidir sobre a imputação ao utilizador. No sentido de considerar que a repartição do prejuízo até ao limite de 50 euros dá-se nos casos de negligencia leve do utilizador, *vide* BENJAMIN GEVA, "Payment Transactions Under the EU Second Payment Services Directive (PSD2) – An Outsider's View", *in Texas International Law Journal*, n.º 2, vol. 54, 2019, disponível em https://digitalcommons.osgoode.yorku.ca (11.04.2021), p. 233. Por sua vez, isto é o que melhor se articula com a nova previsão de que o utilizador não é responsável até o limite referido se este não poderia ter detetado a apropriação do seu instrumento de pagamento antes da realização da operação não autorizada. Para que tal possa suceder, implica, necessariamente, como apontou PATRÍCIA GUERRA em "A realização de operações de pagamento não autorizadas...", cit, pp. 41-42, que o utilizador "agiu com zelo, prudência e diligência", não lhe podendo ser associado qualquer culpa leve e, por isso, não pode ser obrigado a suportar perdas. Parecendo equacionar uma repartição objetiva das perdas, *vide* MARIA RAQUEL GUIMARÃES, "(Ainda) a responsabilidade pelo uso indevido...", cit., pp. 429-430. Ainda no âmbito da al. a), do n.º 2, do art. 115.º, REINHARD STEENNOT, em "Reduced payer's liability...", cit., p. 962, em referência à DSP2, acredita que a não responsabilização do utilizador será de se aplicar mesmo nos casos de negligência grosseira, o que choca com o nosso raciocínio atrás referido. Porém, não nos parece, e salve melhor opinião, que as situações previstas no n.º 2 do normativo sejam de se aplicar quando o utilizador foi grosseiramente negligente, pois não é esta a ideia que se retira da sistematização do art. 74.º da DSP2, que nos diz que o primeiro parágrafo do n.º 1, idêntico ao nosso art. 115.º, n.º 1, não se aplica naquelas duas situações concretas e só seguidamente, no terceiro parágrafo, prevê a responsabilidade

de cuidado com negligência grosseira[154], o mesmo continua a ser responsável até ao limite do seu saldo ou da linha de crédito associada à conta. Em idênticos moldes aos de anteriormente, o utilizador é integralmente responsável se incumprir deliberadamente esse dever ou se atuar fraudulentamente. Por outro lado, mantém-se uma responsabilidade civil obrigacional, derivada do incumprimento dos deveres que o PSP está vinculado pelo contrato, como será o caso em que o prestador não impede que novas operações não autorizadas se realizem depois do utilizador ter comunicado as anteriores e aqueles em que o PSP não forneceu meios adequados para o utilizador poder realizar essa comunicação[155]. Nestes dois casos, o prestador será inteiramente responsável pelas perdas decorrentes das operações não autorizadas[156]. A juntar-se ao leque de instâncias de incumprimento previstas pelo RSP, encontra-se a recente imputação da responsabilidade ao PSP quando este não aplique autenticação forte do cliente[157]. A introdução desta norma terá bastante relevância em casos de fraude realizados com a utilização de cartões de pagamento na Internet e na transferência de fundos através da banca eletrónica. Esta introdução não deixa de suscitar questões. Primeiramente, parece-nos, em consonância com o que acontece com as obrigações acima descritas, que no incumprimento deliberado da obrigação de aplicar autenticação forte nos casos previstos no art. 104.º, a responsabilidade do prestador dar-se-á a título obrigacional, por incumprir um dever acessório à prestação principal a que está adstrito. A dúvida levanta-se nas situações em que o prestador do serviço fez uso das isenções previstas nas NTR/NAC e, por isso, não aplicou uma autenticação reforçada ao utilizador. As isenções previstas permitem ao prestador isentar o utilizador de um procedimento mais demorado de autenticação, de modo a permitir um uso prático e eficiente dos serviços, mas não impõem que o mesmo aplique essas isenções.

---

ilimitada do utilizador no caso de negligência grosseira. Do art. 115.º também se consegue aferir a mesma ideia, pela expressa desaplicação do n.º 1, omitindo-se em relação aos demais números. Se assim não fosse, poderíamos concluir o mesmo para os casos em que o utilizador incumpre as suas obrigações de forma deliberada ou age fraudulentamente.

[154] O novo RSP continua a remeter para o direito nacional a definição de negligência grosseira, o que choca com o intento de uma harmonização total da DSP2. Porém, a DSP2 tenta orientar os Estados sobre em que poderá consistir essa censurabilidade. Veja-se o considerando 72 da DSP2 que nos diz que "a negligência grosseira deverá significar mais do que mera negligência, envolvendo uma conduta que revela um grau significativo de imprudência; por exemplo, conservar as credenciais utilizadas para autorizar uma operação de pagamento juntamente com o instrumento de pagamento, num formato que seja aberto e facilmente detetável por terceiros." Em matéria de negligência grosseira, a DSP2 permitiu aos Estados-Membros limitar a responsabilidade nesses casos, sendo que o nosso RSP preceitua que o utilizador será responsável até ao limite do seu saldo ou da linha de crédito associada à conta mesmo que superior a 50 euros. Não se percebe, por outro lado, porque o legislador português optou por não prever os critérios definidos na Diretiva para que a responsabilidade possa ser limitada, que pressupõe ter-se em conta a natureza das credenciais de segurança personalizadas e as circunstâncias específicas da perda, furto ou apropriação abusiva do instrumento de pagamento, à semelhança da opção tomada também pelo anterior RSP. A DSP2 só dá abertura aos Estados-Membros para reduzirem a responsabilidade do utilizador tendo em conta as circunstâncias referidas, pelo que é importante fazer uma interpretação corretiva e não concluir pela automática aplicação do n.º 4, do art. 115.º, a todos os casos de negligência grosseira. Caso contrário, o tratamento dos utilizadores poderá configurar-se bastante diverso entre os diferentes Estados, veja-se, por exemplo, a opção do legislador italiano, que não fez uso da permissão da DSP2 e previu a responsabilidade ilimitada do utilizador grosseiramente negligente. Cfr. *Decreto Legislativo 27 gennaio 2010, n. 11,* alterado pelo *Decreto Legislativo del 15 dicembre 2017, n. 218*.

[155] Cfr. art. 111.º, n.º 1, al. c) e e) e art. 115.º, n.º 7 e 8. A considerar a responsabilidade obrigacional do prestador, *vide* FRANCISCO MENDES CORREIA, "Operações não autorizadas e o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica", *in Estudos de Direito Bancário I*, CORDEIRO, António Menezes; GOMES, Januário da Costa; BASTOS, Miguel Brito; LEAL, Ana Alves (Coord.), Coimbra, Edições Almedina, 2018, p. 362.

[156] Não é difícil compreender que as perdas que se verifiquem após a comunicação do utilizador ou por impossibilidade de a proceder por falta de meios fornecidos para o efeito, vinculem o PSPGC, uma vez que as mesmas estão ligadas aos fundos depositados na conta e ao PSIP não compete bloquear a utilização da conta *online*. Apesar disso, parece-nos que após ser comunicado da operação não autorizada, deverá abster-se de iniciar pagamentos até que se volte a regularizar o procedimento de autenticação do utilizador.

[157] V. art. 115.º, n.º 5.

Cabe, a cada PSPGC, ponderar e deliberar sobre os custos e benefícios da não aplicação da autenticação forte. É por tal ausência de autenticação derivar de uma decisão e ponderação pessoal do prestador que tendemos a assumir que o mesmo continua a ser responsável pelas perdas quando a não aplicação da autenticação dá-se ao abrigo de umas das isenções previstas[158]. Subjacente a esta ideia está a mesma que prevê a responsabilidade do prestador no caso de operações não autorizadas não imputáveis a nenhuma das partes e nos casos em que ao utilizador é apenas imputável a perdas até ao limite de 50 euros, onde se reparte o remanescente pelo PSPGC[159]. Nestes casos, a responsabilidade do prestador contende com a distribuição do risco, configurando-se como uma responsabilidade objetiva, uma vez que o prestador é aquele que cria e controla a atividade – e o risco que dela advém – que desenvolve em seu benefício. Mas mais importante, como assinala Francisco Mendes Correia, está em causa "uma política legislativa", com o objetivo de incrementar e tutelar a confiança dos utilizadores no bom funcionamento do mercado de pagamentos e com isto incentivar a melhoria da segurança dos serviços por parte dos prestadores[160]. As alterações introduzidas pela DSP2 surgem, precisamente, com o intento de fortalecer a confiança dos consumidores no comércio eletrónico e no sistema de pagamentos que o serve, pelo que a responsabilidade pelo prestador em casos de inexistência de autenticação forte e dinâmica não pode deixar de se afirmar nas isenções previstas.

Já teve a EBA oportunidade de considerar que o PSIP deverá beneficiar das mesmas isenções à autenticação que o utilizador[161], pelo que sugere que a responsabilidade do PSPGC deverá ser de se aplicar nos casos em que a operação, isenta de autenticação, é iniciada pelo PSIP. Questiona-se se a responsabilidade do PSPGC não deveria ser de se conciliar com a eventual imputação ao PSIP de qualquer conduta censurável, isto é, se naquela operação também não se verificou uma deficiência técnica ou falha da sua parte que, nos termos gerais, permitiriam responsabilizá-lo contratualmente perante o utilizador. Atenta-se que, no caso de ser o utilizador a incumprir um dos seus deveres, ainda que deliberadamente, tal não afasta a responsabilidade do PSPGC quando este não aplique a autenticação. Posto isto, do espírito dos normativos pode-se retirar a aceção segundo a qual o utilizador não concorre na distribuição das perdas quando ao PSPGC é de se apontar alguma vicissitude[162]. Em relação ao PSIP, a mesma possibilidade não é difícil de se compreender quando o PSPGC não estava isento de aplicar a autenticação, mas o mesmo já não se pode dizer nos casos em que responde objetivamente, embora, outro sentido não parece emanar do RSP. Ainda assim, a imputação de um facto que permitiu a operação não autorizada deveria ser suficiente para quebrar o nexo de causalidade entre os riscos da atividade do PSPGC e as perdas sofridas pelo utilizador, como

[158] Defendendo que o PSPGC deverá ser igualmente responsável nos casos de isenção de autenticação forte, *vide* GIOVANNI BERTI DE MARINIS, "La disciplina dei pagamenti non autorizzati...", cit., pp. 651-653 e REINHARD STEENNOT, "Reduced payer's liability...", cit., p. 960.
[159] V. art. 115.º, n.º 1.
[160] A considerar a responsabilidade pelo risco do PSP, *vide* FRANCISCO MENDES CORREIA, "Operações não autorizadas...", cit., pp. 373-374 e PATRÍCIA GUERRA, "A realização de operações de pagamento não autorizadas...", cit., pp. 33-35, embora, neste último caso, a Autora parece considerar que estaremos sempre perante uma responsabilidade objetiva, mesmo nos casos em que o prestador incumpriu os deveres do art. 111.º.
[161] EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on the implementation of the RTS* (…), cit., p. 4.
[162] Neste sentido, FRANCISCO MENDES CORREIA, "Operações não autorizadas...", cit., p. 370.

acontece nos casos em que as mesmas lhe possam ser imputáveis[163]. Não se encontrará na desculpabilização da responsabilidade do PSIP as mesmas razões que subjazem à proteção da posição do utilizador perante a ausência de autenticação, pelo que não se compreende porque não esclareceu o regime sobre a possibilidade de responsabilizar o PSIP quando as perdas são imputáveis a conduta sua mesmo no caso de ausência de autenticação.

Nesta linha, importa introduzir e indagar sobre a responsabilidade do PSIP. De acordo com os n.º 2 e 3 do art. 113.º e n.º 9 do art. 114.º, se a operação tiver sido iniciada através do PSIP e o utilizador negue ter autorizado a mesma, cabe logo ao primeiro provar que, na sua esfera de competências, a operação de pagamento foi "autenticada e devidamente registada, e não foi afetada por qualquer avaria técnica ou por outra deficiência" do seu serviço, porém, tal não é "necessariamente suficiente, por si só," para provar que a operação foi mesmo autorizada ou que o utilizador incumpriu com dolo ou negligência grosseira as suas obrigações. Isto diz-nos que, embora as obrigações do art. 110.º digam respeito a instrumentos de pagamento que estão diretamente relacionados com a sua conta de pagamento e que se cumprem perante o PSPGC, o PSIP poderá basear-se nelas para afastar a sua responsabilidade[164]. Do mesmo modo, e em consonância com o que a doutrina vinha defendendo[165], cabe ao PSIP e ao PSPGC, "apresentar elementos que demonstrem a existência de fraude, dolo ou de negligência grosseira da parte do utilizador", não ditando expressamente a quem cabe, primeiramente, desenvolver esse esforço. Porém, no caso de disputa entre o PSIP e o PSPGC, caberá, como já se disse, ao primeiro cumprir o ónus referido no art. 113.º, n.º 2, de modo a alocar a mesma tarefa ao PSPGC perante o utilizador[166], pelo que poderá, neste mesmo momento, indicar os elementos que lhe fazem suspeitar da conduta do utilizador, em consonância com a possibilidade do art. 114.º, n.º 6, mas tal não surge como necessário para o PSIP afastar a sua responsabilidade em juízo. Em relação ao utilizador, essa eventual disputa entre prestadores não implica com a tutela da sua posição, uma vez que o PSPGC está obrigado a reembolsá-lo imediatamente, nos termos do art. 114.º, n.º 5, o que vem afastar a possibilidade do PSPGC adiar o reembolso do utilizador com base na incerteza de que nenhum erro técnico ocorreu na esfera do PSIP[167]. Se se apurar que o PSIP é responsável ou se não conseguir cumprir o ónus da prova que lhe compete, nasce a obrigação de indemnizar o utilizador. Mas, considerando que este já foi reembolsado pelo PSPGC, caberá a este último sub-rogar-se[168] na titularidade do direito que cabia ao utilizador, exigindo do PSIP o

[163] ANTUNES VARELA, a propósito da responsabilidade pelo risco prevista para os acidentes causados por veículos no art. 505.º do CC, considera que a culpa de terceiro exclui a responsabilidade objetiva pelo facto do dano deixar de ser um efeito adequado do risco, *vide* JOÃO DE MATOS ANTUNES VARELA*, Das Obrigações em Geral*, Vol. I, 10.ª Ed, Coimbra, Edições Almedina, 2017, p. 675.

[164] Nada obsta a que as obrigações do art. 110.º respeitantes à segurança dos instrumentos de pagamento sejam cumpridas perante o PSIP quando este oferece um instrumento de pagamento (*v.g.* aplicação de telemóvel que permite a iniciação de pagamentos tanto na Internet como em pontos físicos), mas que, por força da limitação prevista no art. 106.º, n.º 3, al. e), não poderá armazenar credenciais de segurança que permitem o acesso à conta de pagamento. Ainda assim, o cuidado deverá ser sempre de se exigir, dada a possibilidade de haver iniciação de operações sem autenticação.

[165] *Vide* MARIA RAQUEL GUIMARÃES, "(Ainda) a responsabilidade pelo uso indevido...", cit., p.139.

[166] Neste sentido, *vide* MARY DONNELLY, "Payments in the Digital Market…", cit., p. 834.

[167] *Vide* BENJAMIN GEVA, "Payment Transactions Under the EU…", cit., pp. 229-230.

[168] A sub-rogação pelo PSPGC no direito ao reembolso está prevista expressamente na lei pelo n.º 8 do art. 114.º, que visa compensar "o sacrifício que o terceiro chamou a si com o cumprimento". *Vide* JOÃO DE MATOS ANTUNES VARELA*, Das Obrigações em Geral*, Vol. II, cit., 336. Como atenta o Autor, os direitos do sub-rogado (aqui o

pagamento dos montantes entregues ao utilizador e o ressarcimento por outros danos[169]. Encontramos, assim, nos casos em que o PSPGC aplique autenticação forte do cliente, uma nova limitação à sua responsabilidade objetiva, já não contendente com a culpa do lesado, mas com a conduta de um terceiro prestador.

Nesta sede não podemos deixar de considerar discutível a opção do legislador por não distribuir o risco pelos dois prestadores intervenientes no processo. No caso de uma operação não autorizada que não seja imputável a nenhum dos intervenientes, isto é, decorrente de um esquema fraudulento sofisticado e impercetível pelo utilizador[170], o PSIP não será responsável pela mesma, enquanto que, o PSPGC continua obrigado a reembolsar o utilizador, por força da responsabilidade objetiva a que está vinculado nos termos do RSP. Sucede que a atividade do PSIP implica também a exposição do utilizador a novos e acrescidos riscos, mesmo que não detenha fundos do último, pelo que não se configura excessivo que concorresse para a tutela do utilizador, ainda que fora dos casos em que não responde por danos resultantes da sua conduta, mas que não deixam de decorrer da sua atividade, dado que este contribui para a existência e execução da operação, não obstante a solicitação não ter advindo do titular da conta. Reconhece-se, porém, que a opção do legislador é razoável atendendo ao facto de ser o PSPGC o único a quem é permitido deter e gerir fundos dos clientes. Por outro lado, os possíveis ataques e intromissões fraudulentas, que possam ocorrer nas sessões de comunicação também contenderão com a *interface* que é desenvolvida pelo PSPGC e também se compreende que, apesar de se poder dar uma apropriação indevida das credenciais de segurança mediante a solicitação de dados diretamente do utilizador por quem se arroga como o PSIP ou através da clonagem perfeita da sua plataforma onde o utilizador introduz os seus dados de pagamento sensíveis, não pressupõe que as operações não autorizadas que decorrem dessa apropriação indevida se iniciam posteriormente através do PSIP, podendo o terceiro não autorizado aceder diretamente pelo *homebanking* do utilizador e excluir, assim, a iniciação através do terceiro prestador do processo[171].

PSPGC) medem-se em função do cumprimento, pelo que o PSPGC só poderá, a este título, exigir o que entregou ao utilizador. Por sua vez, o preceito faz referência ao dever do PSIP indemnizar os danos sofridos pelo PSPGC, porém, se esses danos ultrapassarem o que este último despendeu para indemnizar o utilizador, já terá de exigir o seu ressarcimento nos termos gerais da responsabilidade civil.

[169] GIOVANNI BERTI DE MARINIS entende que o PSPGC poderá, desde logo, exigir ao PSIP a quantia paga ao utilizador pela operação não autorizada e que, por sua vez, o PSIP, após ter reembolsado o PSPGC, poderá provar a inexistência de qualquer deficiência na sua esfera de competência que o responsabilize pela operação, exigindo de volta o entregue ao PSPGC. Reconhecemos que esta lógica é a que melhor se articula com o disposto no n.º 6, do art. 114.º, ao prever que o PSPGC não deverá proceder ao reembolso imediato do utilizador se o PSIP tiver suspeitas de fraude por parte do utilizador, o que pressupõe que, após a comunicação do utilizador e antes do reembolso do mesmo, os PSP comuniquem entre si e esta comunicação poderia ser, desde logo, a exigência pelo PSPGC de indemnização pelos danos ou do montante a pagar ao utilizador. Apesar disso, esta posição parece invocar fluxos e transferências desnecessários, como não se harmoniza com a exigência da lei de que o PSIP tenha de ser responsável para que o PSPGC possa exigir os montantes entregues ao utilizador. Para que se apure a responsabilidade do PSIP é necessário que este não consiga cumprir o ónus da prova que lhe recai por força dos arts. 113.º, n.º 2 e 114.º, n.º 9. *Vide* GIOVANNI BERTI DE MARINIS, "La disciplina dei pagamenti non autorizzati...", cit., pp. 643-646.

[170] Mesmo em casos de operações fraudulentas, o utilizador pode vir a ser responsável se incumprir os seus deveres de cuidado, mas aqui referimo-nos às situações em que nada lhe é imputável como será o caso das situações subsumíveis à al. a), do n.º 2, do art. 115.º.

[171] Sobre as práticas fraudulentas de *pharming* e *phishing*, *vide* MARIA RAQUEL GUIMARÃES, "O phishing de dados bancários...", cit., pp. 418-422.

Ainda assim, a introdução de um novo interveniente abre portas ao desenvolvimento de fraude distinta dos contornos que hoje conhecemos e implica uma maior dificuldade do controlo dos padrões de qualidade e segurança de todos os intervenientes pelas instituições e pelas autoridades nacionais competentes. Certo é que a tutela do consumidor não sai fragilizada, pelo menos não diretamente, com a solução apresentada pelo legislador, mas a não distribuição do risco pelo PSIP poderá consubstanciar na ligeireza da sua conduta, em comparação com o PSPGC que, por lhe recaírem novos e pesados deveres, tenderá a ser mais cauteloso.

4. Conclusão

Aqui chegados, é evidente a presença constante de uma preocupação por parte do legislador: a tutela da posição do utilizador dos serviços de pagamento que assume frequentemente o papel de consumidor e de titular de dados pessoais perante o acesso à sua conta de pagamento, que conserva informações relevantes e abriga fundos depositados pelo mesmo. Com a sociedade cada vez mais digital, automatizada e acelerada, verificou-se a transferência de serviços tradicionais como é prestação de serviços de pagamento dos balcões presenciais das instituições de crédito para as plataformas eletrónicas de inovadas instituições de pagamento que deixam de ter, muitas vezes, contacto presencial com os consumidores. Esta realidade é, como vimos, nuclear na prestação de serviços de iniciação, pelo que chamou uma imperativa intervenção do legislador na sua regulamentação.

Por sua vez, a abertura das contas de pagamento convoca, não só novas exigências de defesa do utilizador e de segurança nos pagamentos, como também a proteção e limitação do acesso e conservação dos dados do utilizador por terceiros prestadores, com vista ao respeito pela sua privacidade. Neste aspeto, encontra-se uma certa quebra na articulação do RSP com o RGPD, que vem exigir o consentimento expresso para o tratamento de dados pessoais do utilizador sem que o defina e sem atender às regras postuladas no RGPD, uma vez que segundo este último diploma o fundamento desse tratamento é a execução do contrato celebrado. É de reconhecer-se que no âmbito da atividade dos serviços de iniciação, a imperatividade da limitação dos dados a que os prestadores podem ter acesso e a proibição de conservação de dados sensíveis de pagamento é um reforço da posição do utilizador e da sua autodeterminação. Por outro lado, há uma certa ambiguidade relativamente à importância que se dá às credenciais de segurança personalizadas do utilizador e à partilha das mesmas, uma vez que, embora esteja o terceiro prestador proibido de as armazenar, não as deixa de poder recolher. Apesar disso, caberá ao PSPGC determinar o modo de autenticação pelo que, sendo este o principal destinatário dos deveres do RSP, estará mais interessado em adotar o redireccionamento da autenticação. Por outro lado, a definição de dados sensíveis de pagamento não é densificada, nem se pode concluir pela coincidência com o conceito de dados sensíveis plasmado no RGPD.

A grande aposta do novo regime é a obrigação de aplicação da autenticação forte do utilizador, mas esta só alcançará o efeito pretendido se for aplicada por quem gere a conta. Embora a lei não o determine, a EBA considerou que as isenções previstas nas normas técnicas são de se aplicar mesmo quando há acesso de terceiros. Esta posição retira algum efeito prático à importância que se deu à autenticação forte nas situações em que a mesma mais se torna necessária, isto é, nas operações realizadas pela Internet e com o recurso aos serviços de terceiros.

É de se destacar um incremento na proteção do utilizador no que tange com a fraude nos pagamentos eletrónicos, tanto pelo facto de deixar de utilizar os dados de um instrumento de pagamento diretamente na página do comerciante, bem como pela afirmação da responsabilidade do PSPGC pelas perdas resultantes de operações não autorizadas mesmo no caso em que tenha havido o recurso a serviços de iniciação. A lei não vem permitir que o reembolso do utilizador fique dependente de uma eventual disputa sobre a responsabilidade entre os dois prestadores. Ainda assim, o amparo da posição do utilizador é primordialmente assegurado por quem já se encontrava vinculado às regras plasmadas na lei, uma vez que a mesma nada diz em relação a uma repartição objetiva entre o PSIP e o PSPGC.

Regista-se o marco de um novo paradigma no sistema dos serviços de pagamento, tanto pelo reforço da posição do utilizador e da segurança nos pagamentos eletrónicos, bem como pela afirmação de uma autodeterminação da gestão por parte do mesmo no que diz respeito aos fundos depositados junto de outros prestadores. Mas não se pode deixar de notar que o RSP deposita grande confiança no PSIP por partir do pressuposto que os requisitos apertados de autorização, registo e seguro de responsabilidade civil são suficientes para construir uma garantia sólida perante o utilizador. Como a realidade demonstrou relativamente ao setor bancário, isso não é suficiente para afastar a probabilidade de operações fraudulentas por intromissão ou quebra dos seus sistemas.

Apesar das fragilidades que se pode apontar, o novo RSP vem, sem dúvida, melhorar o panorama existente na vigência da lei que transpôs a anterior Diretiva, que deixou de poder acompanhar a evolução tecnológica que se verificou, tanto no que respeita com a inovação dos serviços como pela sofisticação dos métodos fraudulentos. Não é difícil descortinar que a possibilidade de uma semelhante situação se venha a verificar na próxima década, uma vez que o legislador tratou de definir de forma bastante rigorosa os traços que caracterizam a iniciação do pagamento, bem como não concedeu grande espaço, dentro do que discrimina consistir os serviços de pagamento, para a inclusão de novas atividades. Ainda assim, é inerente ao Direito acompanhar a realidade e não a antecipar.

Referências bibliográficas

AUTORIDADE BANCÁRIA EUROPEIA, *Orientações sobre a segurança dos pagamentos efetuados através da internet* (EBA/GL/2014/12_Rev1), 2014, disponível em https://www.eba.europa.eu (20.08.2020)

BAIRROS, RITA MAFALDA VERA-CRUZ PINTO, "A transferência a crédito – Notas caracterizadoras no contexto SEPA e do Regime Jurídico dos Serviços de Pagamento", *in Cadernos O Direito – Temas de Direito Bancário I,* n.º 8, Coimbra, Edições Almedina, 2014, pp. 247-345

BANCO CENTRAL EUROPEU, Parecer do Banco Central Europeu de 5 de fevereiro de 2014 sobre uma proposta de Diretiva do Parlamento Europeu e do Conselho relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2013/36/UE e 2009/110/CE e revoga a Diretiva 2007/64/CE, CON/2014/9, 2014, disponível em https://www.ecb.europa.eu (25.10.2019)

BARREIRA, CAROLINA FRANÇA, "Home banking: A Repartição dos prejuízos decorrentes de fraude informática", *in RED – Revista Eletrónica de Direito*, n.º 3, Porto, CIJE/FDUP, 2015, disponível em https://www.cije.up.pt/pt/red (20.10.2019)

BRENER, ALAN, "Payment Service Directive II and Its Implications", *in Disrupting Finance. FinTech and Strategy in the 21st Century,* Palgrave Pivot, Cham, 2019, pp. 103-117, disponível em https://link.springer.com, pp. 105-108

COMISSÃO EUROPEIA, *Livro Verde – Para um mercado europeu integrado dos pagamentos por cartão, por Internet e por telemóvel*, COM(2011) 941 final, Bruxelas, 2012, disponível em https://www.ec.europa.eu (04.03.2020)

CORDEIRO, A. BARRETO MENEZES, *Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019*, Coimbra, Edições Almedina, 2020

CORREIA, FRANCISCO MENDES, "DSP 2 e Normas Abertas de Comunicação Comuns e Seguras", *in FinTech II: Novos Estudos sobre Tecnologia Financeira*, CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Coord.), Coimbra, Edições Almedina, 2019, pp. 157-166

CORREIA, FRANCISCO MENDES, "Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento" *in III Congresso de Direito Bancário*, VASCONCELOS, L. Miguel Pestana de (Coord.), Coimbra, Edições Almedina, 2018, pp. 385-404

CORREIA, FRANCISCO MENDES, "Operações não autorizadas e o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica", *in Estudos de Direito Bancário I*, CORDEIRO, António Menezes; GOMES, Januário da Costa; BASTOS, Miguel Brito; LEAL, Ana Alves (Coord.), Coimbra, Edições Almedina, 2018, pp. 353-381

CORREIA, FRANCISCO MENDES, *Moeda Bancária e Cumprimento: o cumprimento das obrigações pecuniárias através de serviços de pagamento*, Coimbra, Edições Almedina, 2017

DONNELLY, MARY, "Payments in the Digital Market: Evaluating the contribution of Payment Services Directive II", *in Computer Law and Security Review*, vol. 32, n.º 6, Elsevier Ltd., 2016, pp. 827-839, disponível em https://www.sciencedirect.com (29.11.2019)

DUARTE, DIOGO PEREIRA; GUSEINOV, ALEXANDRA, "O direito de portabilidade de dados pessoais", *in FinTech II: Novos Estudos sobre Tecnologia Financeira*, CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Coord.), Coimbra, Edições Almedina, 2019, pp. 105-127

EIDE, JON STIAN GULBRANDSEN, HALLUM, STIAN, "PSD2: A Strategic Perspective on Third-Party Payment Service Providers", dissertação de mestrado, Oslo, BI Norwegian Business School, 2018 (inédita)

EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC,* EBA/OP/2020/10, 2020, disponível em https://www.eba.europa.eu (22.08.2020)

EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2,* EBA-Op-2019-06, 2019, disponível em https://www.eba.europa.eu (4.10.2019)

EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC* (EBA-OP-2018-04), 2018, disponível em https://www.eba.europa.eu (17.05.2020)

EUROPEAN BANKING FEDERATION, *Guidance for implementation of the revised Payment Services Directive – PSD2 Guidance*, 2.ª Versão, 2019, disponível em https://www.ebf.eu (4.10.2020)

EUROPEAN CENTRAL BANK, "Sixth Report on Card Fraud", 2020, disponível em https://www.ecb.europa.eu (24.08.2020)

FARIA, JOSÉ MANUEL, "Acesso a contas bancárias por terceiros no âmbito de operações de pagamento", *in Revista da Banca*, n.º 71, Lisboa, Associação Portuguesa de Bancos, 2011, pp. 25-39

GEVA, BENJAMIN, "Payment Transactions Under the EU Second Payment Services Directive (PSD2) – An Outsider's View", *in Texas International Law Journal*, n.º 2, vol. 54, 2019, disponível em https://digitalcommons.osgoode.yorku.ca (11.04.2021)

GOMES, M. Januário da Costa, *Contratos Comerciais*, Coimbra, Edições Almedina, 2012

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*, WP259 rev. 01, 2018, disponível em https://www.edpb.europa.eu (8.05.2020)

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações sobre o direito à portabilidade dos dados,* WP242 ver. 01, 2017, disponível em https://www.edpb.europa.eu (21.07.2020)

GUERRA, PATRÍCIA, "A realização de operações de pagamento não autorizadas e a tutela do utilizador de serviços de pagamento em face do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica", *in RED - Revista Eletrónica de Direito*, n.º 2, Porto, CIJE/FDUP, 2016, disponível em https://www.cije.up.pt/pt/red (27.09.2019)

GUIMARÃES, MARIA RAQUEL, "The transposition of PSD2: Decree-Law 91/2018 of 12 November, the Portuguese experience and what may (or may not) change", *in L'attuazione della seconda direttiva sui servizi di pagamento e "open banking"*, a cura di E. Bani, A. Sciarrone Alibrandi, V. de Stasio, Bergamo, Bergamo University Press/Sestante Edizioni, 2021, pp. 141-166

GUIMARÃES, MARIA RAQUEL, "Pagamentos electrónicos não autorizados e fraudulentos", [*in Cibercriminalidade: novos desafios, ofensas e soluções (em revisão)*, I. Guedes & M. Gomes (Eds.), Lisboa, PACTOR – Edições de Ciências Sociais, Forenses e da Educação] (em curso de publicação)

GUIMARÃES, MARIA RAQUEL, "O comércio electrónico ‹‹está na moda››? Algumas questões jurídicas a propósito da oferta de moda ‹‹online››", *in Fashion Law: Direito da Moda,* CASTRO, João Fraga de (Coord.), Cizur Menor, Thomson Reuters Aranzadi, 2019, pp. 827-859

GUIMARÃES, MARIA RAQUEL, "O phishing de dados bancários e o pharming de contas. Análise Jurisprudencial", *in III Congresso de Direito Bancário*, VASCONCELOS, L. Miguel Pestana de (Coord.), Coimbra, Edições Almedina, 2018, pp. 385-404

GUIMARÃES, MARIA RAQUEL, "Os Contratos-Quadro de Prestação de Serviços de Pagamento", *in I Congresso de Direito do Consumo*, CARVALHO, Jorge Morais (Coord.), Coimbra, Edições Almedina, 2016, pp. 177-188

GUIMARÃES, MARIA RAQUEL, "(Ainda) a responsabilidade pelo uso indevido de instrumentos de pagamento eletrónicos em operações presenciais e à distância. Análise do regime introduzido pelo Anexo I do Decreto-Lei n.º 317/2009, de 30 de Outubro (RSP), e das alterações que se perspectivam face à Proposta de Directiva do Parlamento Europeu e do Conselho, de 24 de Julho de 2013", *in I Congresso de Direito Bancário*, VASCONCELOS, L. Miguel Pestana de (Coord.), Coimbra, Edições Almedina, 2015, pp. 115-144

GUIMARÃES, MARIA RAQUEL "The debit and credit card framework contract and its influence on European legislative initiatives", *in InDret Comparado, Revista para el Análisis del Derecho*, n.º 2, 2012, disponível em http://www.indret.com/es (24.09.2020)

GUIMARÃES, MARIA RAQUEL DE ALMEIDA GRAÇA SILVA, *O Contrato-Quadro no Âmbito da Utilização de Meios de Pagamento Eletrónicos*, Coimbra, Wolters Kluwer/Coimbra Editora, 2011

GUIMARÃES, MARIA RAQUEL, "El pago mediante tarjetas de crédito en el comercio electrónico. Algunos problemas relativos a su naturaleza jurídica, marco contractual y régimen aplicable, desde una perspectiva comparada en los Derechos portugués, español y comunitario" (tradução de DOMÍNGUEZ LUELMO, Andrés), *in Los medios electrónicos de pago — Problemas jurídicos*, MATA Y MARTÍN, Ricardo M. (dir.) / JAVATO MARTÍN, Antonio Mª, (coord.), Granada, Editorial Comares, 2007, pp. 167-217

HELGADOTTIR, DILJA, "The interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players", *in Trinity College Law Review,* Vol. 23, 2020, pp. 199-224

LEITÃO, LUÍS MANUEL TELES DE MENEZES, *Direito Das Obrigações*, Volume III, Coimbra, 12.ª Ed., Edições Almedina, 2018

LIMA, RAQUEL SOFIA RIBEIRO DE, "A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa", *in RED – Revista Eletrónica de Direito*, n.º 3, Porto, CIJE/FDUP, 2016, disponível em https://www.cije.up.pt/pt/red (20.10.2019)

MARINIS, GIOVANNI BERTI DE, "La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2", *in Riviste Diritto della banca e del mercato finanziario*, 4/2018, Pisa, Pacini Editore SRL, 2018, pp. 627-655.

MOREIRA, TIAGO CORREIA; BARROS, INÊS ANTAS DE; ORNELAS, ISABELA, "Partilha de dados pessoais e operação bancária aberta", *in Fintech II: Novos Estudos sobre Tecnologia Financeira*, CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Coord.), Coimbra, Edições Almedina, 2019, pp. 147-156

MURRAY, ANDREW, *Information Technology Law: The Law & Society*, 4.ª Ed., Oxford, Oxford University Press, 2019, pp. 439-445

PEREIRA, TIAGO DA CUNHA, "DSP2: Oportunidades e Desafios", *in Revista de Direito Financeiro e dos Mercados de Capitais*, n.º 5, Vol. I, 2019, pp. 507-524, disponível em https://www.blook.pt/home (29.01.2020)

PINTO, Carlos Alberto da Mota, *Teoria Geral Do Direito Civil*, Coimbra, 2.ª Reimp. da 4.ª Ed., Coimbra Editora, 2012

ROCHA, FRANCISCO CHILÃO, "DSP 2 e RGPD: Uma dicotomia nas suas parecenças. Uma visão portuguesa sobre assunto", *in Revista de Direito Financeiro e dos Mercados de Capitais*, vol. 2, n.º 9, 2020, pp. 355-367, disponível em https://www.blook.pt/home (02.10.2020)

ROSALINO, HÉLDER, "FinTech e banca digital", *in FinTech: Desafios da Tecnologia Financeira,* CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Coord.)*,* Coimbra, Edições Almedina, 2017, pp. 9-15

SANTAMARIA, JAVIER, "La segunda Directiva de Servicios de Pago y sus impactos en el mercado", *in Observatorio de Divulgación Financiera,* Nota Técnica n.º 31*,* Instituto de Estudios Financieros, 2018, disponível em https://www.iefweb.org (27.09.2019)

STEENNOT, REINHARD, "Reduced payer's liability for unauthorized payment transactions under the second Payment Services Directive (PSD2)", *in Computer Law and Security Review,* Vol. 34, Elsevier Ltd., 2018, 954-964, disponível em https://www.sciencedirect.com (25.08.2020)

THE EUROPEAN CONSUMER ORGANISATION, *BEUC's Recommendations to the EDPB on the interplay between the GDPR and PSD2,* BEUC-X-2019-021, Bruxelas, 2019, disponível em https://www.beuc.eu (23.11.2019)

THE EUROPEAN CONSUMER ORGANISATION, *Consumer-Friendly Open Banking: Access to Consumer's Financial Data by Third Parties*, *BEUC-X-2018-082*, Bruxelas, 2018, disponível em https://www.beuc.eu (23.11.2019)

THE EUROPEAN DATA PROTECTION BOARD, *Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR*, 2020, disponível em https://www.edpb.europa.eu (22.05.2021).

THE EUROPEAN DATA PROTECTION BOARD, *EDPB PSD2 Letter*, EDPB-84-2018, Bruxelas, 2018, disponível em https://www.edpb.europa.eu (1.12.2019)

VALCKE, PEGGY; VANDEZANDE, NIELS; VAN DE VELDE, NATHAN, *The Evolution of Third Party Payment Providers and Cryptocurrencies Under the EU's Upcoming PSD2 and AMLD4*, SWIFT Institute Working Paper*,* n.º 2015-001, 2015, disponível em https://swiftinstitute.org (27/03/2021)

VARELA, JOÃO DE MATOS ANTUNES*, Das Obrigações em Geral*, Vol. I, 10.ª Ed, Coimbra, Edições Almedina, 2017

VARELA, JOÃO DE MATOS ANTUNES*, Das Obrigações em Geral*, Vol. II, Almedina, 11.ª Reimp. da 7.ª Ed, Coimbra, Edições Almedina, 2015

WOLTERS, P.T.J, JACOBS, B.P.F, "The Security of access to accounts under the PSD2", *in Computer Law and Security Review,* Vol. 35, n.º 1, Elsevier B.V, 2019, pp. 29-41, disponível em https://www.sciencedirect.com (29.11.2019)

Referências jurisprudenciais

Acórdão do Supremo Tribunal de Justiça de 14 de dezembro de 2016, Proc. 1063/12.1TVLSB.L1.S1, Relator Pinto de Almeida, disponível em http://www.dgsi.pt

Acórdão do Tribunal da Relação de Coimbra de 2 de fevereiro de 2016, Proc. 902/13.4TBCNT.C1, Relator Arlindo Oliveira, disponível em http://www.dgsi.pt

Acórdão do Tribunal da Relação do Porto de 7 de outubro de 2014, Proc. 747/12.9TJPRT.P1, Relator Ana Lucinda Cabral, disponível em http://www.dgsi.pt

(texto submetido a 30.03.2021 e aceite para publicação a 16.05.2021)