U.PORTO

MESTRADO
CIÊNCIAS JURÍDICO-CIVILÍSTICAS

A REVISÃO DA DIRETIVA DOS SERVIÇOS DE PAGAMENTO E A PROTEÇÃO DO UTILIZADOR-CONSUMIDOR

Joana Queiroga

M

2024

RESUMO

O mercado dos serviços de pagamento mudou significativamente nos últimos anos. Fruto da evolução tecnológica, surgiram novos prestadores de serviços financeiros e a consequente partilha de dados financeiros entre bancos e empresas de tecnologia financeira- *open banking*, bem como, novos e mais sofisticados tipos de fraude, com impacto direto nas garantias de proteção e segurança dos utilizadores.

Não obstante a clara evolução legislativa nesta matéria, a avaliação de desempenho da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro, detetou algumas fragilidades deste regime, essencialmente no que respeita a matérias de proteção dos consumidores e de concorrência entre os diferentes prestadores de serviços de pagamento. Assim, de modo a garantir um setor financeiro europeu apto às transformações tecnológicas em curso, em 28 de junho de 2023, a Comissão Europeia apresentou uma proposta de revisão da Diretiva Serviços de Pagamento.

É sobre esta nova proposta legislativa que recairá o nosso estudo, em confronto com atual quadro normativo em vigor- DSP2, sobretudo, no que concerne às garantias de proteção conferidas aos consumidores/utilizadores dos serviços de pagamento.

ABSTRACT

The payment services market has changed significantly in recent years. As a result of technological evolution, new financial service providers have emerged and the consequent sharing of financial data between banks and financial technology companies - open banking, as well as new and more sophisticated types of fraud, with a direct impact on the protection and security guarantees of users.

Notwithstanding the legislative developments in this area, the assessment of the Directive (EU) 2015/2366 of the European Parliament and of the Council, of November 25th, detected some weaknesses in this regime, essentially on the matters of consumer protection and competition between different payment service providers. Therefore, to guarantee a European financial sector capable of ongoing technological transformations, on June 28, 2023, the European Commission presented a proposal to revise the Payment Services Directive.

Therefore, it is this new legislative proposal that our study will focus on, in comparison with the current regulatory framework in force - DSP2, focusing on the protection granted to consumers/users of payment services.

Um especial agradecimento aos meus pais, pelo apoio incondicional. À minha avó, pela inspiração e exemplo, que guardarei para sempre. E à Senhora Prof. Doutora Maria Raquel Guimarães, pela orientação e incentivo.

Porto, 25 de julho de 2024

ÍNDICE

1. INTRODUÇÃO

O advento da internet traduz uma das maiores revoluções do século XX. A Era digital mudou a forma como as pessoas vivem, comunicam e acedem aos mais variados serviços. O presente é digital. A população mundial utiliza cada vez mais serviços através de meios digitais[1]. O mercado dos serviços financeiros não é exceção. O papel central da inovação financeira no século XXI é atribuído ao desenvolvimento de tecnologias de informação e comunicação. Assim, o progresso tecnológico representa hoje um especto importantíssimo no âmbito da competitividade dos prestadores de serviços financeiros tradicionais[2].

O acesso aos serviços financeiros através de meios digitais é hoje uma realidade comum para consumidores e empresas[3]. Nos estabelecimentos comerciais a percentagem de pagamentos efetuados através de meios digitais, e sem contacto, é cada vez maior, e as compras em linha aumentaram significativamente nos últimos anos[4]. Garantir o funcionamento seguro das infraestruturas digitais revela-se essencial para a economia à escala mundial.

De acordo com o Relatório dos serviços de pagamentos do Banco de Portugal, referente ao ano de 2023 "os consumidores portugueses continuam a preferir os instrumentos de pagamento eletrónicos (cartões de pagamento, débitos diretos, transferências a crédito e transferências imediatas.)"[5]. Mantem-se a trajetória de crescimento dos pagamentos em Portugal, impulsionada pela utilização de instrumentos eletrónicos. De acordo com o mesmo relatório, os instrumentos de pagamento eletrónicos foram usados em 99,8% dos pagamentos processados no SICOI (sistema de compensação interbancária), face a 99,7% em 2022, e cresceram 13,5% em quantidade e 14,9% em valor, sendo que os cartões continuaram a ser o

[1] De acordo com o estudo "Digital 2023: *Global Overview Report*", de Simon Kemp, de 26 de janeiro de 2023, 64,4% das pessoas do planeta estão agora online (5.16 mil milhões de utilizadores). Os dados demonstram uma subida de 1,9% no número total. Este total representa um aumento de 3% em 12 meses ou mais 137 milhões de pessoas. Este número tem vindo a crescer de forma progressiva ao longo dos anos, passando de apenas 2,6 milhões em 1990 para 396 milhões em 2000, 1,9 mil milhões em 2010, 4,6 mil milhões em 2020 e para os actuais 5,1 mil milhões. Estudo disponível em <Digital 2023: Global Overview Report — DataReportal – Global Digital Insights> (20-07-2024).

[2] Neste sentido, Inna Romānova, Simon Grima, Jonathan Spiter, e Marina Kudinska, *in* "The Payment Services Directive II and Competitiveness: The Perspective of European Fintech Companies", *in European Research Studies Journal*, Volume XXI, Issue 2, 2018, 3-22 p. 6.

[3] Mafalda Miranda Barbosa, em "Serviços de pagamentos, repartição do risco e responsabilidade civil – algumas reflexões a propósito da nova diretiva dos serviços de pagamentos (DSP2)", in *Revista de Direito Comercia*l, 2017, p. 623.

[4] ACEPI - Associação Portuguesa da Economia Digital, *Economia digital em Portugal – Edição 2022*, pp. 37-41, disponível em <Estudo-da-Economia-e-da-Sociedade-Digital-2022-ACEPI-IDC-PT-Versão-Completa.pdf (computerworld.com.pt)> (11-06-2024).

[5] Banco de Portugal, *Relatório dos Sistemas de Pagamentos - 2023*, Lisboa, 2024, p. 16, disponível em <Relatório dos Sistemas de Pagamentos - 2023 (bportugal.pt)>(09-06-2024).

meio de pagamento mais utilizado[6]. Também os pagamentos com cartão com recurso à tecnologia *contactless*, bem como, as compras online com cartão, registaram crescimento[7].

Este aumento é também registado na União Europeia. O mercado dos serviços de pagamentos eletrónicos movimentou cerca de 240 mil milhões de euros em valor em 2021, em comparação com 184,2 mil milhões de euros referentes ao ano de 2017, continuando em constante crescimento, tanto em número, como em valor de transações[8]. No que respeita ao ano de 2023, 70% dos indivíduos, com idade compreendia entre os 16 e os 74 anos, compraram bens ou serviços através da internet, face a 58% em 2018[9].

Estes dados não deixam margem para dúvidas: a inovação tecnológica está a transformar o mundo, e transformou, radicalmente, o mercado da prestação de serviços financeiro.

O constante desenvolvimento da tecnologia financeira (*FinTech*)[10] e a digitalização e globalização dos serviços financeiros, aumentaram as exigências da regulamentação dos serviços de pagamento ao nível comunitário, com vista à uniformização do quadro regulamentar, vital para o sucesso da economia europeia[11]. O legislador europeu tomou desde cedo consciência da importância que o mercado único de serviços de pagamento assume para o desmantelamento de todas as fronteiras internas da Comunidade[12].

---

[6] Banco de Portugal, *Relatório dos Sistemas de Pagamentos - 2023*, cit., p. 11.

[7] Os pagamentos com cartão com recurso à tecnologia *contactless* cresceram 31,1% em número e 32,7% em valor. Por seu turno, as compras *online* com cartão também continuaram a crescer: aumentaram 35,3% em número e 33,7% em valor- Banco de Portugal, *Relatório dos Sistemas de Pagamentos - 2023*, cit., p. 11.

[8] Comissão Europeia, *Modernizar os serviços de pagamento e abrir os dados relativos aos serviços financeiros: novas oportunidades para os consumidores e as empresas*, de 28 de Junho de 2023, Bruxelas, disponível em <Modernizar os serviços de pagamento e os dados relativos aos (europa.eu)> (06-06-2024). Também quanto aos hábitos de pagamento dos consumidores, *vide*, European Central Bank, *Study on the payment attitudes of consumers in the euro area (SPACE), 2022*, disponível em <Study on the payment attitudes of consumers in the euro area (SPACE) – 2022 (europa.eu)> (26-05-2024).

[9] Eurostat- *Digital economy and society statistics - households and individuals*, 2023, disponível em <Digital economy and society statistics - households and individuals - Statistics Explained (europa.eu)> (26-05-2024).

[10] De acordo como Banco de Portugal "*O termo fintech pode referir-se a entidades que operam no setor financeiro e que têm modelos de negócio baseados em tecnologias inovadoras"*, *Fintech +, o novo canal do Banco de Portugal sobre inovação financeira*, de 23-05-2018, disponível em <Fintech +, o novo canal do Banco de Portugal sobre inovação financeira | Banco de Portugal (bportugal.pt)> (26-05-2024); sobre *Fintech*, *vide,* também, Carlos Moura – "FinTech e regulação no mercado bancário", in *Fintech: desafios da tecnologia financeira* (coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira e Diogo Pereira Duarte), 2.º ed., Coimbra, Almedina, 2019, p. 21.

[11] A este respeito, Maria Raquel Guimarães, "La Directiva (ue) 2015/2366, sobre servicios de pago (DSP2) y los pagos electrónicos", Working paper 3/2022, disponível em <Càtedra Jean Monnet de Dret Privat Europeu (ub.edu)> (26-05-2024), pp. 4 e 5.

[12] O conceito de mercado comum tem a sua origem em 1958, no artigo 2.º da versão original do Tratado de Roma. Tinha por objetivo a liberalização das trocas comerciais entre os Estados-Membros, de forma a "*aumentar a prosperidade económica e contribuir para uma união cada vez mais estreita entre os povos da Europa*", cit., Parlamento Europeu, "O mercado interno: princípios gerais", em *Fichas temáticas sobre a União Europeia*, de Christina Ratcliff, Jordan De Bono e Barbara Martinello, novembro de 2023, disponível em <O mercado interno: princípios gerais | Fichas temáticas sobre a União Europeia | Parlamento Europeu (europa.eu)> (04-05-2024). Do

O primeiro passo legislativo de relevo com vista à uniformização do quadro normativo dos serviços de pagamento na União Europeia, foi dado pelo Parlamento Europeu, em 2007, com a publicação da Diretiva dos Serviços de Pagamento (DSP1) [13]. Até essa data, não obstante os diversos atos comunitário publicados neste domínio[14], os mercados dos serviços de pagamento dos Estados-Membros encontravam-se organizados separadamente, balizados por fronteiras nacionais, com um enquadramento jurídico não harmonizado, compartimentado em 27 regimes jurídicos distintos.

Em 2015, após a análise do impacto da Diretiva 2007/64/CE e a consulta sobre o Livro Verde da Comissão de 11 de janeiro de 2012[15], ocorreu nova revisão no quadro jurídico europeu dos serviços de pagamento[16], através da publicação da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro (Diretiva de Serviços de Pagamento revista, ou DSP2), transposta para o ordenamento jurídico nacional através do Decreto-Lei n.º 91/2018, de 12 de novembro[17]. A segunda Diretiva Serviços de Pagamento visou eliminar os obstáculos

---

Ato único a Maastricht, até ao presente, várias foram as intervenções legislativas na busca por um mercado comum, concorrencial e em plena harmonia com outras temáticas que foram ganhando maior relevo no panorama europeu. Sobre esta evolução histórica, com maior pormenor, Francisco Mendes Correia, em "*Moeda bancária e cumprimento, O cumprimento das obrigações pecuniárias através de serviços de pagamento*", Coimbra, Almedina, 2017, pp. 430-455.

[13] Diretiva 20017/64/CE do Parlamento Europeu e do Conselho de 13 de novembro de 2007, transposta para o Ordenamento Português através do Decreto-Lei n.º 317/2009, de 30 de outubro. Revogada pela Diretiva 2015/2366/UE do Parlamento Europeu e do Conselho, de 25 de novembro.

[14] Nomeadamente, a Diretiva 97/5/CE do Parlamento europeu e do Conselho, de 27 de Janeiro de 1997, relativa às transferências transfronteiras, e o Regulamento (CE) n.o 2560/2001 do Parlamento Europeu e do Conselho, de 19 de Dezembro de 2001, relativo aos pagamentos transfronteiras em euros, que, no entanto, não foram suficientes para colmatar a situação, tal como a Recomendação 87/598/CEE da Comissão, de 8 de Dezembro de 1987, relativa a um código europeu de boa conduta em matéria de pagamento eletrónico (relações entre instituições financeiras, comerciantes-prestadores de serviços e consumidores), a Recomendação 88/590/CEE da Comissão, 17 de Novembro de 1988, relativa aos sistemas de pagamento, em especial no que diz respeito às relações entre o titular e o emissor dos cartões, e a Recomendação 97/489/CE da Comissão, de 30 de Julho de 1997, relativa às transações realizadas através de um instrumento de pagamento eletrónico, nomeadamente em relação às relações entre o emitente e o detentor.

[15] Vieram expor importantes desafios do ponto de vista regulamentar para os quais aquela DSP1 não apresentava soluções claras e adequadas, conforme refere Francisco Mendes Correia, em "*Moeda Bancária e cumprimento das obrigações pecuniárias através de serviços de pagamento*", cit., p. 513. No mesmo sentido, o considerando 4 da DSP2 que aponta para alguma fragmentação do quadro regulamentar do anterior Diploma (DSP1), bem como, para os critérios pouco claros quanto às atividades excluídas do seu âmbito de aplicação.

[16] Sobre a revisão da DSP1, Francisco Mendes Correia, *Moeda Bancária e Cumprimento - O cumprimento das obrigações pecuniárias através de serviços de pagamento*, cit., p. 574 e s.s..

[17] Sobre a transposição da DSP2 para o nosso ordenamento, *vide:* Maria Raquel Guimarães, "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" / The Transposition of PSD2 and Open Banking*, a cura di/(Edd.) E. Bani, V. De Stasio, A. Sciarrone Alibrandi, Bergamo, Sestante Edizioni, 2021, pp. 141-166. Também sobre o tema, Banco de Portugal, *Diretiva dos Serviços de Pagamentos revista (DSP2) foi transposta para o ordenamento jurídico nacional. O que muda?*, disponível em <Diretiva dos Serviços de Pagamentos revista (DSP2) foi transposta para o ordenamento jurídico nacional. O que muda? | Banco de Portugal (bportugal.pt)> (26-05-2024), bem como, *Audição da Comissão de Orçamento, Finanças e Modernização Administrativa (COFMA) -Diretiva dos serviços de pagamento revista (DSP2)*, 15 de Junho de 2018, disponível em <Apresentação do Diretor do Departamento de Serviços Jurídicos, Pedro Machado, e do Diretor do

a novos tipos de serviços de pagamento e melhorar a proteção e segurança dos consumidores[18] apresentando uma série de inovações e aperfeiçoamentos ao quadro normativo da DSP1[19] .

2. EVOLUÇÃO NO DOMÍNIO DA INOVAÇÃO DIGITAL - O CAMINHO ATÉ À PROPOSTA DO NOVO REGULAMENTO

Conforme já referido, as tecnologias no domínio dos mercados de pagamentos estão em constante evolução, acarretando mudanças profundas na indústria dos serviços financeiros, e bem assim, no modo como os consumidores e as empresas acedem a estes serviços[20]. O ato de pagamento, por exemplo, tem vindo a desmaterializar-se de forma acelerada nos últimos anos[21]. A inovação e digitalização continuarão a transformar o modo de funcionamento dos pagamentos, que passarão por novos canais e novas formas de iniciação, como por exemplo, através de os "dispositivos usáveis" (relógios, óculos, cintos, etc.), sendo até expectável, que num futuro próximo, sejam dispensáveis quaisquer tipos de dispositivos e os pagamentos possam ser efetuados através de tecnologias de autenticação avançadas, como as baseadas em biometria[22]. A pandemia covid-19 foi também grande impulsionadora do recurso aos

---

Departamento de Sistemas de Pagamentos, Egrejas Francisco na Comissão de Orçamento, Finanças e Modernização Administrativa sobre Serviços de Pagamento de Moeda Eletrónica (bportugal.pt)> (26-05-2024).

[18] *Vide* considerando 3 da DSP2.

[19] Não no iremos ocupar das alterações introduzidas pela DSP2, mas sobre esta matéria a Doutrina é abundante. Apontamos alguns exemplos: Maria Raquel Guimarães, "La Directiva (ue) 2015/2366, sobre servicios de pago (DSP2) y los pagos electrónicos", cit.; Alberto Franco Pozzolo, "PSD2 and the transformation of the business model of payment services providers"*, in L'attuazione della seconda direttiva sui servizi di pagamento e "open banking" / The Transposition of PSD2 and Open Banking,* A cura di / (Edd.), E. Bani, V. De Stasio, A. Sciarrone Alibrandi, Bergamo, Sestante Edizioni, 2021, pp. 29-42; Tiago da Cunha Pereira, "DSP: Oportunidades e desafios", *in Revista de Direito Financeiro e dos Mercados de Capitais*, Vol. (2019), No.5, 507-524, disponível em <Vol.-1-2019-no.-5-Tiago-da-Cunha-Pereira-DSP2-Oportunidades-e-Desafios.pdf (rdfmc.com)> (05-05-2024). Francisco Mendes, "Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento", *in III Congresso de direito bancário*, Coimbra, Almedina, 2017, pp. 385-404; Francisco Mendes Correia, "Os novos serviços de iniciação de pagamentos: algumas notas sobre a responsabilidade civil", *in Estudos de direito do consumo*, volume II, Rui Mascarenhas Ataíde, Francisco Rodrigues Rocha, Vítor Palmela Fidalgo (org.), Coimbra, Almedina, 2023, pp. 755-771;

[20] Sobre este tema, Ulrich Bindseil, Monika Hempel, "A estratégia do Eurosistema para os pagamentos de retalho/ The Eurosystem retail payments strategy", *in InforBANCA- Revista do Instituto de Formação Bancária*, edição nº 121, janeiro 2021, pp. 11 a 16, disponível em <IFB-InforBanca-121_JAN2021.pdf> (11-06-2024); bem como, Maria Tereza Cavaco, "Pagamentos: o futuro já começou"*, in InforBANCA- Revista do Instituto de Formação Bancária,* edição nº 130, janeiro 2024, pp. 16 a 20, disponível em <InforBanca-130-JANEIRO-2024.pdf (ifb.pt)> (11-06-2024).

[21] Mafalda Miranda Barbosa, em "Serviços de pagamentos, repartição do risco e responsabilidade civil…", in *Revista de Direito Comercia*l, cit., p. 623.)

[22] Neste sentido, a Comissão Europeia na *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre uma Estratégia para os pagamentos de pequeno montante na EU*, COM (2020) 592 final, Bruxelas, 24.9.2020, p. 2 e 3. *Vide* também, *Como a IoT está moldando os modelos de pagamento do futuro*, Giovani Zago, de 31 jan. 2022, disponível em <Como a IoT está moldando os modelos de pagamento do futuro. (linkedin.com)> (09-06-2024). E ainda sobre este tema, Maria Raquel Guimarães, "Mb way, 'engenharia social' e operações fraudulentas", *in Nova Consumer Lab,* 31 de maio de 2021, disponível em <MB Way, "engenharia social" e operações fraudulentas (unl.pt)> (26-05-2024).

pagamentos digitais e veio confirmar a importância vital dos pagamentos seguros, acessíveis e cómodos, nas transações à distância e presenciais.

É certo que inovação tecnológica abarca um sem número de vantagens e oportunidades; no entanto, é também geradora de grandes complexidades, nomeadamente, em termos de conformidade e de supervisão regulamentares[23]. O risco de ciberataques constitui um enorme obstáculo para a estabilidade e alinhamento almejados, representando uma séria ameaça à garantia de segurança do sector financeiro[24]. A criação de um setor financeiro competitivo, passa pela abertura de portas à inovação, sem que, no entanto, seja descurada a garantia de regras de estabilidade financeira e proteção dos consumidores[25].

Em 2018 a transição digital da Europa passou a ser uma das principais prioridades apontadas pela União Europeia para década seguinte[26], tendo sido apresentado o primeiro plano de ação para a tecnologia financeira[27]. Também neste sentido, em 2020, a Comunicação da Comissão sobre a estratégia para os pagamentos de pequeno montante na UE[28], que definiu as prioridades para o sector dos pagamentos de pequeno montante durante o mandato do atual colégio de comissários (2019 – 2024), plano que foi acompanhado de uma Estratégia de Financiamento Digital, definindo-se as prioridades para a agenda digital no setor financeiro, para além dos pagamentos[29].

Ora, foi no âmbito da estratégia para os pagamentos de pequeno montante que foi anunciada uma "avaliação exaustiva da aplicação e do impacto da DSP2". Assim, em 2022, foi efetuada a avaliação *ex post* da DSP2[30]. Em suma, a avaliação identificou um aumento de

---

[23] Neste sentido, a introdução da Comunicação da Comissão de 2018 COM (2018) 109 final, p. 2. Também neste sentido, os resultados da consulta da Comissão Europeia, *Consultation on a retail payments strategy for the EU*, disponível em <2020 - Retail payments strategy - European Commission (europa.eu)> (24-06-2024).

[24] Em 2016, o setor financeiro foi alvo de ciberataques com uma frequência 65% superior à de qualquer outro setor. Fonte: Estudo da IBM, «Security trends in the financial services sector», abril de 2017, *cfr.* nota de rodapé n.º 8 da Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre uma Estratégia em matéria de Financiamento Digital para a EU, COM(2018) 109 final, Bruxelas, 8.3.2018;

[25] COM(2018) 109 final.

[26] *Cfr.* discurso de Charles Michel, presidente do Conselho Europeu, no fórum FT-ETNO, 29 de setembro de 2020;

[27] COM(2018) 109 final - visou a implementação das novas tecnologias no sector financeiro, identificando três temas basilares: permitir aos modelos empresariais inovadores alcançar uma dimensão à escala da UE , apoiar a adoção da inovação tecnológica no setor financeiro, e por fim, reforçar a segurança e a integridade do setor financeiro.

[28] Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, sobre uma Estratégia para os pagamentos de pequeno montante na EU, COM (2020) 592 final, Bruxelas, 24.9.2020.

[29] Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre uma Estratégia em matéria de Financiamento Digital para a EU*, COM (2020) 591 final, Bruxelas, 24.9.2020. *Vide* também Conselho Europeu Conselho da União Europeia, *Finança Digital*, de 04 de março de 2024 disponível em <Finança digital - Consilium (europa.eu)> (24-06-2024).

[30] Para esta avaliação contribuíram um relatório de um contratante independente, bem como, os pontos de vista das partes interessadas no âmbito de várias consultas públicas (Comissão Europeia, *Convite à apreciação de uma*

novos tipos de fraude, questão preocupante no que respeita ao objetivo fundamental de proteção dos consumidores[31]. Foram identificadas insuficiências no que respeita ao objetivo de melhorar o mercado do *open banking*, ao passo que os progressos no sentido de melhorar a prestação de serviços de pagamento transfronteiras também foram limitados, em grande parte, devido a incoerências nas práticas de supervisão e na aplicação da legislação diversa em toda a UE[32]. Foram também identificados fatores que restringem o progresso no que respeita ao objetivo da DSP2 de nivelar as condições de concorrência entre os diferentes PSPs (prestadores de serviços de pagamento)[33]. Estas matérias identificadas no documento de trabalho da Comissão de 2023 vieram assim reclamar por uma reforma ao quadro normativo da DSP2. Embora não seja possível colocar um fim absoluto à fraude, a mesma pode ser reduzida e os seus impactos mitigados. No que concerne ao o*pen banking*, um regime complexo, dispendioso e pouco claro, reclama por simplificação e maior clareza, a par de um aumento dos meios de fiscalização efetiva. Quanto às incoerências e divergências na transposição do quadro legal, bem como, algumas lacunas da DSP2, rogam por nova reforma legislativa, em busca de um quadro mais harmonioso, menos ambíguo, que acarrete maior clareza e segurança jurídica ao almejado mercado único[34].

Assim, em resposta ao resultado da avaliação *ex post* da DSP2, em 28 de junho de 2023, a Comissão Europeia apresentou um pacote de medidas relativas à alteração da DSP2, que inclui uma proposta de Diretiva relativa aos Serviços de Pagamento e aos serviços de moeda eletrónica, centrada na concessão de licenças e na supervisão das instituições de pagamento[35], bem como, uma proposta de Regulamento relativo aos serviços de pagamento da UE[36].

---

avaliação e de uma avaliação de impacto realizadas em paralelo, Ref. Ares(2022)3556263, de 10/05/2022, disponível em <Serviços de pagamento — revisão das normas da UE (europa.eu)> (26-05-2024)), de acordo com os quais, a DSP2 registou diferentes graus de sucesso na prossecução dos fins a que se propunha, sendo que, de um modo geral, a DSP2 permitiu progressos de valor acrescentado, concluindo pela relativa eficiência no que respeita aos custos, não obstante, algumas insuficiências identificadas- *vide* texto introdutório da PRSP e European Commission, "Commission staff working document, Impact assessment report, accompanying the documents Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 and Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC, SWD(2023) 231 final, Brussels, 28.6.2023, disponível em <EUR-Lex - 52023SC0231 - EN - EUR-Lex (europa.eu)> (19-07-2024) final, p.6.

[31] SWD(2023) 231 final, pp. 8 a11.

[32] Idem, pp. 12 a 18.

[33] Idem, pp. 18 a 19.

[34] Idem, p. 21.

[35] Proposta de Diretiva do Parlamento Europeu e do Conselho relativa aos serviços de pagamento e aos serviços de moeda eletrónica no mercado interno que altera a Diretiva 98/26/CE e revoga as Diretivas (UE) 2015/2366 e 2009/110/CE, COM(2023) 366 final, Bruxelas, 28.6.2023.

[36] Proposta de Regulamento do Parlamento Europeu e do Conselho relativo aos serviços de pagamento no mercado interno e que altera o Regulamento (UE) n.º 1093/2010, COM(2023), 367 final Bruxelas, 28.6.2023.
on payment services in the internal market and amending Regulation (EU) No 1093/2010 COM (2023) 367 final

A proposta de atualização da Diretiva dos serviços de pagamento (DSP3) e o Regulamento dos serviços de pagamento (PRSP) procuram revolucionar o quadro jurídico dos serviços de pagamento, visando garantir um sector ágil e apto a acompanhar os avanços tecnológicos deste mercado[37].

É sobre as alterações propostas ao quadro jurídico dos pagamentos de retalho na União Europeia (UE) que recairá o nosso estudo. Nesta medida, de seguida analisamos as principais alterações com acolhimento no novo quadro legal dos serviços de pagamento, previstas na proposta de Regulamento de serviços de pagamento, fazendo o devido contraponto com o regime atual em vigor da Diretiva (EU) 2015/2366. (*)

3. PROPOSTA DE REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO — PRSP— QUAL O FUTURO?

3.1. HARMONIZAÇÃO DA EXECUÇÃO E APLICAÇÃO NOS ESTADOS-MEMBROS

A avaliação do impacto e da aplicação da Diretiva (EU) 2015/2366, levada a cabo pela Comissão Europeia, identificou, desde logo, questões relacionadas com a aplicação divergente nos diferentes Estados destinatários[38]. Esta falta de coerência na aplicação do quadro jurídico da DSP2 conduziu a que fossem criadas condições regulamentares nacionais diferentes, com impacto direto na concorrência entre os prestadores de serviços de pagamentos. Ora, é em

---

[37] *Cfr.* Marta Graça Rodrigues e Tomás Gomes da Silva, em *Futuro do setor dos pagamentos na União Europeia: análise das novas propostas regulatórias*, de 27-10-2023, disponível em <Futuro do setor dos pagamentos na União Europeia: análise das novas propostas regulatórias | Garrigues> (15-07-2024); Laura Chaney e Vicenzo Renda, "*How to Design a Successful European Payments Market? DIGITALEUROPE's position on the Payment Services Regulation (PSR) and Payment Services Directive 3 (PSD3) Proposals*" *in Digital Europe*, 17-11-2023, disponível em <Payment-Services-Regulation-PSR-position-paper.pdf (digitaleurope.org)>(26-05-2024); Sébastien Bianco, *How do PSD3 and PSR impact the EU payments sector?,* de 19-04-2024, disponível em <How do PSD3 and PSR impact the EU payments sector? - Powens>(20-07-2024), e ainda, Lavan Thasarathakumar e Virginia Montgomery, *Evolution not revolution: European Commission publishes financial data access and payments package*, de 30-06-2023, disponível em <Evolution not revolution: European Commission publishes financial data access and payments package - Hogan Lovells Engage> (18-07-2020)

* Tratando-se de um processo Legislativo em curso, na presente data, após parecer do Comité Económico e Social Europeu e da Comissão dos Assuntos Económicos e Monetários, o Parlamento apresentou, em sede de primeira leitura em processo legislativo ordinário, proposta de alteração à PRSP: Parlamento Europeu, P9_TA(2024)0298, Serviços de pagamento no mercado interno e alteração do Regulamento (UE) n.º 1093/2010 - *Resolução legislativa do Parlamento Europeu, de 23 de abril de 2024, sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo aos serviços de pagamento no mercado interno e que altera o Regulamento (UE) n.º 1093/2010* (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)), disponível em <TA (europa.eu)> (16-07-2024). Não obstante, aguarda-se ainda pela posição do Conselho Europeu até que seja conhecida a proposta legislativa a adotar - e consequentes alterações. Nestes termos, debruçamos o nosso estudo sobre a proposta da Comissão, com necessária referência às propostas de alteração apresentadas pelo Parlamento Europeu.

[38] SWD(2023) 231 final, p. 16.

relação a esta matéria que surge uma das principais inovações do novo quadro normativo proposto pelo legislador europeu, conforme veremos mais à frente.

O facto de os Estados Membros procederem à transposição da Diretiva de forma pouco homogénea, conjugada, muitas vezes, com a falta de robustez dos direitos e deveres aplicados, foram apontados como fatores que limitaram o progresso dos objetivos da DSP2[39]. Por exemplo, atualmente, a DSP2 concede grande discricionariedade no que respeita ao regime sancionatório a aplicar pelos Estados-Membros[40]. Acrescem ainda, os diferentes poderes conferidos às autoridades nacionais de supervisão, assim como, as dificuldades apresentadas pelas mesmas no que respeita à concreta aplicação das sanções em causa, quer por falta de recursos, quer por falta de competências específicas para supervisionar[41]. Nesta medida, podemos mesmo referir uma espécie de lacuna de supervisão, uma vez que, não existem entidades competentes disponíveis para o efeito. Não sendo errado referir que não existe uma concreta garantia do cumprimento das regras de defesa do consumidor, tendo em conta que, não se encontra acautelada a competente fiscalização nesse sentido.

A falta de harmonização legislativa nos diferentes Estados-Membros reflete-se também nos requisitos de licenciamento dos PSPs, prazo do processo de candidatura, bem como, nos requisitos regulamentares de operações transfronteiriças[42], assim como, no que respeita às exclusões consagradas na DSP2, o que levou, inclusive, a que a EBA viesse a adotar orientações sobre o tema[43]. A escassez de uniformização na transposição da DSP2 pelos diferentes Estados-Membros resulta na falta de concorrência equilibrada entre os PSPs, criando condições regulamentares diferentes, o que conduz a uma maior concentração de PSPs em Estados-Membros que apresentam requisitos de licenciamento e supervisão mais favoráveis.

---

[39] *Cfr.* Considerando 4 da PRSP.

[40] Artigo 103.º da DSP2. Esta matéria encontra-se assim assente em disposições de direito nacional administrativo dos Estados-Membros, o que se traduz num processo bastante moroso e pouco uniforme, com regimes mais benevolentes em contraponto com outros mais rígidos e penosos para os infratores- neste sentido ver SWD(2023) 231 final, p. 17.

[41] A título de exemplo, refira-se a incerteza existente no tratamento da exclusão dos prestadores de ATM independentes. A supervisão adequada desta exclusão é colocada em causa, uma vez que, cabe às autoridades de supervisão avaliar se as atividades dos prestadores de ATM independentes são elegíveis como prestação de serviços de pagamento ou se se enquadram na exclusão prevista no artigo 3.º, alínea o), da DSP2. Sucede que, essas atividades e prestadores estão fora do âmbito de aplicação da DSP2 e, por conseguinte, fora da supervisão e da competência das Autoridades competentes.

[42] SWD(2023) 231 final, p. 17.

[43] Ver parecer Autoridade Bancária Europeia (EBA), *Guidelines on the limited network exclusion under PSD2*, (EBA/GL/2022/02), 24 de fevereiro de 2022, disponível em <Final report on draft Guidelines on the limited network exclusion under PSD2.pdf (europa.eu)> (26-05-2024).

Nestes termos, a reforma legislativa apresentada pela Comissão, procura apresentar uma resposta que passa por uma maior harmonização legislativa, bem como, pelo reforço das disposições sobre sanções.

3.1.1. Harmonização legislativa

Ora, é à luz da problemática exposta que surge uma das principais alterações propostas, que carece desde logo enfatizar: a escolha do instrumento legislativo — um Regulamento, em substituição da Diretiva[44]. Assim, considerou a Comissão adequado consagrar no âmbito de um regulamento as regras aplicáveis às instituições financeiras, de transposição direta para todos os Estados-Membros, a fim de colmatar as divergências na transposição e aplicação da DSP2 nos diferentes ordenamentos jurídicos. Desta forma, a Comissão Europeia pretende colocar termo à procura do "foro mais favorável" por parte dos prestadores de serviços de pagamentos[45]. Iniciativa que nos parece de saudar e para a qual antevemos o sucesso ambicionado. Com este novo instrumento, espera-se maior harmonização do quadro legislativo que rege os serviços de pagamento na União Europeia, estabelecendo condições de concorrência mais justas e equilibradas[46].

É de ressalvar, no entanto, que, as regras relativas à autorização e supervisão das instituições de pagamento, continuarão a fazer parte de uma Diretiva, concedendo o legislador neste campo alguma liberdade de atuação aos Estados-Membros. É de referir também, a opção do legislador em agrupar o regime dos serviços de pagamento e o regime de moeda eletrónica, até agora regulados por diplomas distintos – DSP2 e pela Diretiva da moeda eletrónica[47].

De modo a evitar entendimentos divergentes, foi também pretensão do legislador conferir maior clareza e concretização às regras definidas na PRSP (proposta de regulamento

---

[44] O artigo 288.º do Tratado sobre o Funcionamento da União Europeia estabelece que uma diretiva é vinculativa, quanto ao resultado a alcançar nos Estados-Membros destinatários, deixando às instâncias nacionais a competência quanto à forma e aos meios para alcançar o resultado, por seu turno, o Regulamento tem caráter geral. É obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros. Sobre este tema, *vide*, Maria Raquel Guimarães, "«Na minha Conta ou na tua?» Revisitação do Regime aplicável às operações fraudulenta à luz da nova Proposta de um Regulamento relativo aos serviços de pagamento no mercado interno, de Junho de 2023", *in A Revista, Supremo Tribunal de Justiça*, 2024, pp. 65 a 68.

[45] Considerando 4 da PRSP.

[46] Sobre este tema, Maria Raquel Guimarães, em "«Na minha Conta ou na tua?»…", cit., pp. 66 a 68.

[47] À semelhança do que já havia sido feito pelo legislador português em 2012, aquando da transposição da Diretiva da moeda eletrónica e da sua incorporação no RSP1 e, posteriormente, em 2018, com o RSP2. De acordo com o legislador europeu, o "*quadro jurídico aplicável às instituições de moeda eletrónica e às instituições de pagamento, em especial no que diz respeito às regras de conduta da atividade, já está substancialmente harmonizado*". Nesta medida, faz todo o sentido a criação de consonância entre o regime de autorização e supervisão aplicável às instituições de moeda eletrónica e o regime aplicável às instituições de pagamento. Já no que concerne aos requisitos para concessão de licenças, terão de, necessariamente, ser acauteladas as respetivas diferenças e especificidades de cada regime

de serviços de pagamento), de forma a não conceder lugar a interpretações distintas e, bem assim, colmatar algumas lacunas existentes. Neste sentido, o legislador começa agora por elencar as categorias de prestadores de serviços sujeitos às obrigações previstas na PRSP e na PDSP3, o que representa uma novidade face à DSP2[48]. Relativamente às entidades e operações excluídas do escopo deste quadro normativo, existe uma quase total coincidência entre as exclusões previstas na PRSP e as previstas na DSP2, com duas exceções que merecem o nosso reparo: os serviços de levantamento de numerário em caixas automáticas disponibilizadas por prestadores que atuam em nome de um ou vários emitentes de cartões e que não sejam partes no contrato-quadro celebrado com o cliente que efetua o levantamento de dinheiro de uma conta, que se encontravam excluídos do âmbito da DSP2[49]. No entanto, esta exclusão não encontra acolhimento da PRSP. Por outro lado, os serviços de "disponibilização de numerário em estabelecimentos de venda a retalho na sequência de um pedido expresso do utilizador de serviços de pagamento, mas independentemente da execução de qualquer operação de pagamento e sem qualquer obrigação de efetuar uma compra de bens e serviços", representam uma novidade prevista na PRSP[50]. Procura com esta alteração não obstar ao acesso a numerário, permitindo que os comerciantes possam oferecer serviços de disponibilização de numerário, independentemente de qualquer compra por parte do cliente, sem a necessidade de estarem habilitados como prestadores de serviços de pagamentos[51].

3.1.2. Reforço disposições sobre sanções

Qualquer alteração legislativa relevar-se-á inócua se desprovida de uma atividade fiscalizadora da sua correta aplicação e efetivo cumprimento. Nesta medida, o quadro

[48] Artigo 2.º, n.º 1da PRSP. *Vide* considerando 6 da PRSP.
[49] *Cfr.* alínea o) do artigo 3.º da DSP2. Sobre este tema, no âmbito da DSP2, Francisco Mendes Correia, "Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento", cit., pp. 393-394.
[50] Artigo 2.º, n.º 2, alínea E) da PRSP. *Cfr*. considerando 9 da PRSP. Este incremento no regime das exclusões da PRSP prende-se com o facto de se ter revelado difícil, ao abrigo da DSP2, a exclusão a determinadas categorias de operadores de caixas automáticas (ATM). Assim, entendeu o legislador proceder à substituição da categoria de operadores de caixa automáticas, excluídos ao abrigo da DSP2, pela categoria de operadores de caixas automáticas que não gerem contas de pagamento.
[51] Em relação a esta matéria é de referir a proposta de alteração apresentada pelo Parlamento Europeu, em relação aos artigos 7.º e 28.º da PRSP, no sentido de reforçar as informações a prestar aos utilizadores sobre eventuais encargos associados à operação de levantamento de numerário (incluindo taxas de câmbio) — *vide* Parlamento Europeu, P9_TA(2024)0298, Serviços de pagamento no mercado interno e alteração do Regulamento (UE) n.º 1093/2010 — *Resolução legislativa do Parlamento Europeu, de 23 de abril de 2024, sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo aos serviços de pagamento no mercado interno e que altera o Regulamento (UE) n.º 1093/2010* (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)), disponível em <TA (europa.eu)> (16-07-2024).

regulamentar europeu dos serviços de pagamentos clamou pelo reforço de disposições conducentes à efetiva aplicação de sanções perante situações de incumprimento[52].

Nestes termos, à semelhança do já estipulado na DSP2, cabe aos Estados-Membros designar as autoridades competentes para assegurar e acompanhar e cumprimento efetivo do quadro regulamentar referente aos serviços de pagamentos[53], a quem competirá exercer a atividade fiscalizadora de investigar alegadas infrações, bem como, impor sanções e medidas administrativas perante o incumprimento dos prestadores de serviços, dos direitos e obrigações previstas no quadro normativo em vigor[54]. Para o efeito, as autoridades nacionais competentes devem dispor de todos os poderes de investigação e de recursos adequados e necessários para o desempenho das suas funções[55]. De igual modo, caberá aos Estados-Membros prever as sanções e medidas administrativas aplicáveis em caso de infração[56]. O (alargado) critério de definição dessas medidas continua a ser o mesmo fornecido pela DSP2: efetivas, proporcionais e dissuasivas[57].

Até aqui, conforme vimos, existe uma quase total identidade entre o regime previsto na PRSP e DPS2 no que respeito aos critérios para fixação das sanções a aplicar, continuando o legislador a atribuir um alargado critério interpretativo e de aplicação aos diferentes Estados-Membros. Sucede que, de forma a dar resposta às insuficiências já elencadas[58], o legislador europeu veio concretizar um conjunto de infrações específicas sobre as quais recairá a obrigatoriedade de serem consagradas medidas sancionatórias, perante a sua violação ou evasão[59], fixando também as medidas e sanções administrativas aplicáveis às infrações elencadas[60]. No mesmo sentido, o legislador vem concretizar os elementos a considerar na determinação das sanções em causa[61]. Esta alteração legislativa vem colocar cobro a um

[52] Foi também neste sentido o *feedback* recebido pela Comissão Europeia no âmbito da consulta pública realizada para a avaliação do impacto de aplicação da Diretiva (UE) 2015/2366, tendo sido apontadas insuficiências nos regimes de execução dos Estados-Membros, *cfr.* SWD(2023) 231, *Annex II: Stakeholder consultation*.
[53] Artigo 91.º, n.º 2 da PRSP e artigo 100.º, n.º 1 da DSP2.
[54] Considerando 124 da PRSP.
[55] Artigo 91.º, n.º 1 da PRSP e artigo 100.º, n.º 3 da DSP2. Na eventualidade de as autoridades competentes deleguarem o exercício dos seus poderes noutras autoridades ou organismos nos termos da alínea c) do artigo 91.º n.º 1, a delegação de poderes deve especificar as funções delegadas, bem como, as condições em que devem ser realizadas e as condições em que a delegação de poderes pode ser revogada.
[56] Na PRSP o legislador vem acrescentar que os Estados-Membros podem optar por não estabelecer regras em matéria de sanções ou medidas administrativas aplicáveis a infrações desde que estas estejam já sujeitas ao seu direito penal nacional. Nesse caso, os Estados-Membros devem dar conhecimento à Comissão Europeia das disposições de direito penal aplicáveis e quaisquer alterações subsequentes das mesmas, em conformidade com o artigo103.º- *cfr.* previsto no n.º 2 do artigo 96.º da PRSP.
[57] Artigo 96.º, n.º 1 da PRSP e artigo 103.º n.º 1 da DSP2.
[58] Neste sentido o considerando 132 da PRSP.
[59] Artigo 97.º da PRSP.
[60] Artigo 97.º, n.º 2 da PRSP.
[61] Considerando 128 da PRSP. O artigo 99.º da PRSP elenca os elementos a considerar.

critério demasiado alargado de discricionariedade conferida aos Estados-Membros, propício a regimes pouco harmonizados.

Com vista a conferir maior poder às decisões das autoridades nacionais competentes, a PRSP vem consagrar o direito de as autoridades competentes imporem sanções pecuniárias compulsórias, a pessoas singulares ou coletivas, por incumprimento de qualquer decisão, injunção, medida provisória, solicitação, obrigação ou outra medida adotada[62], estabelecendo os valores de referência mínimos a aplicar, possibilitando, no entanto, que os Estados-Membros definam montantes mais elevados[63].

Quanto aos procedimentos para tratamento e resolução das reclamações dos utilizadores de serviços de pagamento, por violação das obrigações a que estejam sujeitos os PSPs, a proposta de Regulamento não apresenta qualquer alteração ao regime em vigor. Em suma, recai sobre os PSPs o ónus de estabelecerem e aplicarem os procedimentos adequados para tratamento e resolução das reclamações apresentas pelos utilizadores, sempre sobre o estrito acompanhamento das autoridades nacionais competentes[64].

O RSP procura agora, como meio dissuasor de práticas de incumprimento, incentivar a cooperação entre as autoridades competentes, através da partilha de informação entra Estados-Membros, em matéria das sanções impostas aos PSPs, sempre que essas informações se mostrem relevantes para outras autoridades[65]. No mesmo sentido, estabelece que as autoridades competentes devem publicar, nos seus *websites,* todos os casos que resultem na aplicação de uma sanção ou medida administrativa específica, por violação do (futuro) RSP, com a salvaguarda de que, sendo o infrator uma pessoa singular, a sua identidade não poderá ser revelada[66]. Com esta iniciativa o legislador procura que a partilha de informações entre Estados-Membros possa servir como um alerta quanto à conduta do prestador de serviços de pagamento infrator, assim como, um instrumento dissuasor, para que outros prestadores de serviços de pagamento não incorram no mesmo comportamento infrator.

No cômputo geral, a PRSP não aparenta consagrar alterações substanciais no que respeita ao reforço das disposições sancionatórias, bem como, não apresenta uma solução de

[62] Considerando 133 da PRSP.
[63] Artigo 98.º, n.º 1 da PRSP.
[64] Artigo 94.º da PRSP e artigo101.º da DSP2: é fixado o prazo de 15 dias úteis para resposta às reclamações, salvo situações excecionais, que justifiquem um prazo mais alargado, sem nunca exceder o prazo de 35 dias úteis. Salvaguarda-se que os Estados-Membros podem introduzir ou manter regras relativas aos procedimentos de resolução de litígios que sejam mais vantajosas para o utilizador de serviços de pagamento, conforme já previsto da DSP2.
[65] De acordo com o considerando 129 da PRSP as autoridades de supervisão devem ter conhecimento das debilidades dos prestadores de serviços de pagamento em matéria de cumprimento das regras do Regulamento.
[66] Artigo 101.º da PRSP.

raiz para garantir coerência na atividade fiscalizadora e sancionatória dos diferentes Estados-Membros. É apresentado um regime em muito semelhante ao contemplado na DSP2, que continuará a resultar numa aplicação divergente em matéria de sanções, consoante o Estado-Membro em que as infrações venham a ser praticadas. Não obstante o legislador vir definir os critérios relativos a sanções e medidas administrativas a aplicar e, bem assim, elencar um conjunto de sanções administrativas e outras medidas relativas a infrações específicas, certo é que, todo o quadro normativo concede ampla liberdade de decisão aos Estados-Membros. Ora, sendo o objetivo do legislador a harmonização do quadro normativo sancionatório, não nos parece que tenha sido feliz nas alterações apresentadas, que, certamente, ficarão aquém do objetivo ambicionado.

3.2. REFORÇO DA PROTEÇÃO DOS UTILIZADORES E A CONFIANÇA NOS PAGAMENTOS

A fraude representa um dos principais receios dos utilizadores no que concerne à utilização de serviços pagamentos através de meios digitais[67]. No entanto, de acordo com o relatório do Banco de Portugal referente ao ano de 2023[68], os níveis de fraude na utilização de instrumentos de pagamento revelam-se muito reduzidos, sendo que se verificou que as fraudes mais comuns resultaram de mecanismos de engenharia a social[69], como é o caso do *phishing*[70], em que existe apropriação das credenciais de segurança dos utilizadores ou dos elementos de autenticação forte dos clientes, fornecidas pelos próprios utilizadores, atuando os infratores em

[67] A consulta pública realizada no âmbito da revisão da DSP2 revela que 17% dos inquiridos (11 em 66) afirmam ter sido vítimas de fraude recentemente. Desses 11, 4 solicitaram o reembolso junto do PSP e receberam integralmente. Por outro lado, 3 dos entrevistados indicaram ter efetuado o pedido, no entanto, não receberam o reembolso. Neste sentido o resultado da consulta publica efectuada- ver SWD (2023) 231 final, p. 19.

[68] Banco de Portugal, *Relatório dos Sistemas de Pagamentos - 2023*, cit., p.12.

[69] De acordo com o European Payments Council, "*a engenharia social é um vetor de ataque que explora o erro humano para obter informações privadas, acesso ou objetos de valor"(...)"um método de persuasão pelo qual, através de uma variedade de técnicas, um atacante manipula as pessoas para realizar ações que levam a comprometimento ou fraude*" *in* (EPC183-22), *2022 Payment Threats and Fraud Trends Report, novembro de 2022*, p. 14, disponível em <2021 Payments Threats and Fraud Trends Report (europeanpaymentscouncil.eu)> (24-06-2024).

[70] O *phishing* é uma técnica fraudulenta que se traduz no envio em massa de mensagens de correio eletrónico tendo como objetivo a obtenção de dados que permitam aceder às contas bancárias das vítimas através do serviço de *home banking*, *cfr*, Maria Raquel Guimarães em "A fraude no comércio electrónico: o problema da repartição do risco por pagamentos fraudulentos" cit., p. 583, nota 10; ou, de acordo com o Acórdão so Supremo Tribunal de Justiça de 18.12.2013: "*O phishing (do inglês fishing, «pesca») pressupõe uma fraude electrónica caracterizada por tentativas de adquirir dados pessoais, através do envio de emails com uma pretensa proveniência da entidade bancária do receptor, por exemplo, a pedir determinados elementos confidenciais (número de conta, número de contrato, número de cartão de contribuinte ou qualquer outra informação pessoal), por forma a que este ao abri-los e ao fornecer as informações solicitadas e/ou ao clicar em links para outras páginas ou imagens, ou ao descarregar eventuais arquivos ali contidos, poderá estar a proporcionar o furto de informações bancárias e a sua utilização subsequente (...)*".

nome dos verdadeiros titulares para iniciar e validar as operações de pagamento[71]. Também o relatório do *European Payments Council*[72], elaborado em 2022, sobre as ameaças de pagamentos e tendências de fraude, aponta no mesmo sentido: o principal foco da fraude passa pelos ataques de engenharia social, *phishin*g e tentativas de *vishing*, muitas vezes em combinação com *malware*[73].

Para a redução dos níveis de fraude, em muito contribuiu a grande inovação trazida pela DSP2: a implementação do mecanismo de autenticação forte, isto é, a autenticação através da conjugação de dois ou mais meios de autenticação[74]. Foi isso que concluiu a avaliação levada a cabo pela Comissão, referindo que a implementação do mecanismo de autenticação forte foi um fator de sucesso no que respeita ao combate à fraude[75]. No entanto, também os mecanismos de fraude encontram mudança com a evolução tecnológica, adaptando-se a cada nova tendência e desenvolvendo novos esquemas, cada vez mais sofisticados.

As situações de fraude para as quais a autenticação forte não representa um mecanismo eficaz, prendem-se muitas vezes com a falsificação de identidade, como é o caso dos ciberataques ou roubos de instrumento de pagamento, cenário em que um burlão efetua o pagamento, substituindo-se ao ordenante genuíno. Assim como, as "fraudes reembolso", em que a fatura/recibo é intercetada por uma terceira pessoa, que altera o IBAN da conta de destino

---

[71] Em 2023, os PSP reportaram ao Banco de Portugal 48 incidentes de caráter severo (menos sete do que no ano de 2022). Desses, 45 foram de natureza operacional e 3 de segurança, resultantes de ações maliciosas levadas a cabo por agentes externos. Os 48 incidentes ocorridos afetaram cerca de 2,1 milhões de utilizadores e levaram à não execução de 2,2 milhões de transações, no valor de 146 milhões de euros (975 milhões de euros em 2022) – Banco de Portugal, *Relatório dos Sistemas de Pagamentos - 2023*, cit., p.12.

[72] European Payments Council, *2022 Payment Threats and Fraud Trends Report,* cit., p. 14.

[73] "*Malware, abreviação de software malicioso, é um termo genérico usado para se referir a uma variedade de formas de software hostil ou intrusivo. Os cibercriminosos projetam malware para comprometer funções de computação, roubar dados, ignorar controles de acesso e causar danos a computadores host, dispositivos de clientes e seus aplicativos ou dados",* European Payments Council, *2022 Payment Threats and Fraud Trends Report,* cit., p.16

[74] O Artigo 97.º do DSP2 exige que os PSP apliquem o SCA (strong customer authentication) sempre que o ordenante aceda a uma conta de pagamento em linha, inicie uma operação de pagamento digital ou realize qualquer ação através de um canal remoto que possa implicar um risco de fraude no pagamento ou outros abusos. Sobre a autenticação forte (SCA) no âmbito da DSP2, *vide*, Simone Mezzacapo, "PSD2, online and mobile payments: what transparency for the future of payments?"*, in L'attuazione della seconda direttiva sui servizi di pagamento e "open banking" / The Transposition of PSD2 and Open Banking*, A cura di / (Edd.), E. Bani, V. De Stasio, A. Sciarrone Alibrandi, Bergamo, Sestante Edizioni, 2021, pp. 98 a 106; Maria Raquel Guimarães,, "Pagamentos electrónicos não autorizados e fraudulentos", *in Cibercriminalidade: novos desafios, ofensas e soluções*, PACTOR - Edições de Ciências Sociais, Forenses e da Educação, 2021, p. 231; também, em Maria Raquel Guimarães, em "La Directiva (ue) 2015/2366, sobre servicios de pago (DSP2) y los pagos electrónicos", cit., pp. 12 e 13; Lucía Alvarado Herrera, Autenticación reforzada de cliente y responsabilidad en la segunda directiva de servicios de pago, in *Revista de Derecho del Sistema Financiero 5*, Março de 2023, pp. 69-112.

[75] É isto que resulta da consulta pública efetuada pela Comissão: "*Respondents also find that SCA has helped to make digital payments safer and more secure (50 replies, 76%)"* – SWD(2023) 231 final, p. 64. Bem como, Iván Nablón, *"La identificación electrónica: redefiniendo las reglas del sector financiero*", Papeles de Economía Española, n.º 162, 2019, 162-174, p.169.

para a qual deveria ser promovido o pagamento[76], levando a que seja o próprio cliente a realizar o pedido de transferência a partir do seu dispositivo, com a respetiva autenticação. Os esquemas de pagamento autorizados não são apenas mais difíceis de detetar, são também mais difíceis de gerir, quando detetados. A par destas situações, surgem também fraudes mais sofisticadas, de pagamentos designados pela sigla APP (*Authorised Push Payments*), que envolvem engenharia social, em que o ordenante é manipulado de forma a crer que está perante um beneficiário genuíno, ou mesmo, perante um representante de um banco[77]. Nestes casos (*phishing*, *vishing*, *smishing*, *spoofing*, etc.), facilmente se explica a inoperância da autenticação forte, uma vez que, a maioria destas transações fraudulentas foram efetivamente autorizadas pelo ordenante genuíno. O consumidor pensa que está a enviar dinheiro para o destinatário real, quando, na verdade, está a enviar para um terceiro[78].

A avaliação levada a cabo à DSP2 concluiu também que existe uma área cinzenta no que respeita à isenção de aplicação do SCA (strong customer authentication)[79]. A DSP2 não oferece clareza sobre esta matéria, designadamente, sobre se alguns tipos de transações são incluídos ou excluídos da aplicação do SCA. É o caso de *mail orders* ou *telephone orders* (MOTOs) e de *merchant Initiated Transactions* (MITs)[80]. Os MIT estão implicitamente excluídos do SCA pelo facto de o artigo 97.º, n.º 1, do PSD2 aplicar o SCA a três ações realizadas pelo ordenante, sem mencionar quaisquer ações iniciadas pelo beneficiário, facto que veio a ser confirmado pela Comissão numa sessão de perguntas e respostas da EBA[81]. Já no que se refere às MOTO, de acordo com o considerando 95 da DSP2, não se revelou necessário "garantir o mesmo nível de proteção às operações de pagamento iniciadas e executadas com modalidades diferentes da utilização de plataformas ou dispositivos eletrónicos, como as operações de pagamento em papel, encomendas por correio ou por telefone"[82]. De acordo um com parecer da EBA, a exclusão da aplicação do SCA para

[76] *Cfr.* refere Maria Raquel Guimarães, em "«Na minha Conta ou na tua?»…", cit., p. 106.
[77] European Payments Council, *2022 Payment Threats and Fraud Trends Report,* cit., p. 40.
[78] Maria Raquel Guimarães, em "«Na minha Conta ou na tua?»…", cit., p.106.
[79] Autoridade Bancária Europeia (EBA), *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, (EBA/Op/2022/06), de 23 de junho de 2022, p.76, 84 e 85, disponível em <EBA's response to the Call for advice on the review of PSD2.pdf (europa.eu)> (26-05-2024).
[80] SWD(2023) 231 final, pp. 10 e 11.
[81] Autoridade Bancária Europeia (EBA), *Aplicabilidade do SCA a 'pagamentos por cartão iniciados apenas pelo beneficiário*, Q&A 2018_4031, de 01 de março de 2019, disponível em <2018_4031 Applicability of SCA to 'card payments initiated by the payee only' | European Banking Authority (europa.eu)> (26-05-2024).
[82] A este respeito foram fornecidas algumas orientações nos Q&A promovidos pela EBA: *Strong customer authentication and common and secure communication (incl. access)*, *Q&A 2018_4058,* de 01 de Março de 2019, disponível em <2018_4058 Transactions initiated via Interactive Voice Response (IVR) solutions | European Banking Authority (europa.eu)> (26-05-2024); *Q&A 2019_4788*, de 12 de março de 2021, disponível em <2019_4788 Treatment of electronic bookings similar to Mail Order and Telephone Orders (MO-

operações de pagamento não digitais revelou-se difícil de aplicar e de supervisionar na prática, uma vez que, com base na formulação do considerando, apenas os pagamentos em numerário ficariam fora do âmbito do SCA, sendo que, todos os outros tipos de operações de pagamento seriam, em alguma parte da execução do pagamento, tratados eletronicamente[83] .

Conforme já mencionado, a avaliação da aplicação da Diretiva (UE) 2015/2366, efetuada pela Comissão, concluiu que a autenticação forte do cliente se revelou bastante eficaz no combate à fraude, representando um enorme passo nesse sentido. Atendendo à eficácia já comprovada, a autentificação forte não deve ser contornada[84].

3.2.1. **A autenticação forte**

A PRSP, à semelhança da DSP2, exige a autenticação forte do cliente[85] sempre que este "aceda em linha à sua conta de pagamentos", "emita uma ordem de pagamento para uma operação de pagamento eletrónico", ou "realize uma ação, através de um canal remoto, que possa envolver um risco de fraude no pagamento ou outros abusos", acrescentando a necessidade de autenticação forte para os casos em que o utilizador "aceda a informações sobre contas de pagamento" [86].

TO) transactions | European Banking Authority (europa.eu) > (26-05-2024); e *Q&A 2019_4790*, de 12 de março de 201, disponível em <2019_4790 Keyed Mail Order or Telephone Order (MO-TO) transactions | European Banking Authority (europa.eu)> (26-05-2024).

[83] Autoridade Bancária Europeia (EBA), *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, cit., pp. 75 e 76.

[84] Memorando 108 da PRSP. Neste sentido conforme veremos mais à frente, o legislador faz recair sobre o prestador de serviços de pagamento a responsabilidade pelas perdas financeiras no âmbito de operações em que este não exige autenticação forte do cliente. Entende-se que este normativo acarreta um efeito dissuasor ao contorno da aplicação do mecanismo de autenticação forte.

[85] À luz da PRSP, a autenticação forte do utilizador é definida como "*uma autenticação baseada na utilização de dois ou mais elementos pertencentes às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é), os quais são independentes, na medida em que a violação de um deles não compromete a fiabilidade dos outros, e que é concebida de modo a proteger a confidencialidade dos dados de autenticação*". De acordo com a Resolução legislativa do Parlamento Europeu (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)), a aplicação de autenticação dever basear-se na avaliação dos riscos, para que os consumidores possam beneficiar de uma autenticação forte do cliente ininterrupta e capaz de assegurar uma ferramenta eficaz na luta contra a fraude, *cfr.* considerando (107-A) do citado diploma. Em relação a este tema, o Banco Central Europeu recomenda a alteração do regulamento proposto no sentido de clarificar que os PSPs devem aplicar a autenticação forte do cliente utilizando, pelo menos, dois elementos independentes de categorias diferentes, *cfr. Parecer do Banco Central Europeu de 30 de abril de 2024 sobre uma proposta de Regulamento e de Diretiva relativa aos serviços de pagamento e de moeda eletrónica,(CON/2024/13), C/2024/3869 de 19.6.2024, disponível em* <C_202403869PT.000101.fmx.xml (europa.eu) *(16-07-2024).*

[86] Artigo 85.º da PRSP e artigo 97.º da DSP2. Embora a Comissão tenha acrescentado a necessidade de autenticação forte para os casos em que o utilizador "*aceda a informações sobre contas de pagamento*" na PRSP, o Parlamento Europeu propõe no âmbito da Resolução legislativa (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)), cit., a exclusão dessa alínea, mantendo o texto em vigor na DSP2; não obstante, nos termos do artigo 89.º n.º 1 da PRSP, é igualmente aplicável a autenticação forte nos termos do artigo 85.º, n.º 10, caso os pagamentos sejam iniciados através de um prestador de serviços de iniciação de pagamentos e sempre que as informações sejam solicitadas através de um prestador de serviços de informação sobre contas.

Ao legislador cabe a difícil tarefa de garantir a mitigação dos caminhos que possibilitem o contorno deste mecanismo de segurança, através da clarificação de conceitos e maior concretização do regime, o que desde logo ressalta do extenso corpo do normativo referente a esta matéria previsto na PRSP, face ao que vigora no âmbito da DSP2.

Nesta senda, a PRSP procurou agora clarificar as definições de "operações iniciadas pelos comerciantes (MIT)[87] e de ordens postais ou telefónicas (MOTO)"[88], de forma a não permitir que os PSPs, de modo "encapotado", justifiquem a não aplicação da autenticação forte do cliente. A PRSP clarifica assim que, no que respeita às MIT, a autenticação forte do cliente deve ser aplicada no momento do estabelecimento do mandato inicial*,* afastando a necessidade de a aplicar a subsequentes operações de pagamento iniciadas pelo comerciante[89]. Por seu turno, em relação às MOTO, clarifica a PRSP que apenas as operações de iniciação de pagamentos devem ser não digitais para que uma operação seja considerada uma MOTO (e não a sua execução), e, portanto, esteja afastada a obrigação de aplicar a autenticação forte do cliente[90]. Deste modo, delimitando-se com maior clareza o âmbito das operações em causa, menor será a abertura a diferentes interpretações e, por conseguinte, para contorno da aplicação da autenticação forte do cliente.

Por seu turno, no que respeita às operações de pagamento eletrónicas remotas[91], o legislador continua a determinar que a autenticação forte a aplicar deve incluir elementos que associem de forma dinâmica a operação a um montante e beneficiário específico[92]. Esta associação do pagamento a um montante e beneficiário específico reforça a segurança na

[87] Em consonância com e recomendação da EBA: EBA/Op/2022/06, n.º s 323 e 324, p. 75 e 76.
[88] Considerando 108 da PRSP, cit.
[89] Idem.
[90] Idem.
[91] De acordo com o artigo 4.º n.º 6 da DSP2, consiste na "*operação de pagamento iniciada através da Internet ou através de um dispositivo que possa ser utilizado para comunicação à distância*". Por seu turno, a PRSP fala em "*iniciação remota de operação de pagamento*", que define como "*uma operação de pagamento para a qual é emitida uma ordem de pagamento através da Internet*", cf. n.º 7 do artigo 3º. A PRSP eliminou assim a referência ao dispositivo que possa ser utilizado para comunicação à distância, de forma a abarcar mais clareza à definição de "operação remotas".
[92] Artigo 85.º n.º 8 e 9 da PRSP, e bem assim, artigo 97.º n.º 2 da DSP2. Por exemplo, através do envio de um código de confirmação da operação para o telemóvel do cliente, a chamada senha de utilização única, *cfr.,* refere Miguel Pestana de Vasconcelos, "A responsabilidade do banco por operações de pagamento não autorizadas no *online banking*, decorrente do novo regime de serviços de pagamento (RSP II)", *in Julgar*, n.º 42, 2020, 191-208, p. 200. Sendo que estes aspetos são depois detalhados no Regulamento delegado (EU) 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.

operação e confere maior transparência, permitindo ao ordenante conhecer a todo o momento os dados da operação[93].

Não obstante o esforço por uma maior concretização dos critérios referentes à autenticação forte, consciente da insuficiência deste mecanismo para, por si só, ser meio suficiente para o combate absoluto à fraude, o legislador vem propor uma novidade no âmbito da PRSP: os PSPs devem passar a dispor de mecanismos de controlo de operações e de partilha de dados relativos a situações de fraude[94]. Estes mecanismos devem ter por base o histórico de pagamentos e de acessos a contas de pagamento em linha, designadamente, informações sobre o utilizador dos serviços de pagamento, nomeadamente, características ambientais e comportamentais que lhe são específicas em circunstâncias de utilização normal das credenciais de segurança personalizadas, informações sobre a conta de pagamento, informações sobre a operação (o montante da operação e o identificador único do beneficiário), bem como, os dados relativos à sessão iniciada, incluindo o intervalo do endereço IP do dispositivo a partir da qual a conta de pagamento foi acedida[95]/[96].

O legislador não descurou também uma análise mais inclusiva[97], e considerando que o acesso a elementos de autenticação poderá não ser acessível por todos, face a eventuais limitações de meios de acesso, ou até mesmo, de conhecimento tecnológico, procurou garantir a proteção proporcionada pela autenticação forte do cliente, a pessoas com deficiência, idosos, pessoas com competências digitais limitadas e pessoas sem acesso a dispositivos digitais, como telemóveis inteligentes[98]. Para o efeito, caberá aos prestadores de serviços de pagamento

---

[93] *Cfr*. refere Maria Raquel Guimarães, em "«Na minha Conta ou na tua?»…", cit., p. 87; bem como, Simone Mezzacapo, *PSD2, online and mobile payments: what transparency for the future of payments?, in L'attuazione della seconda direttiva sui servizi di pagamento e "open banking" / The Transposition of PSD2 and Open Banking*, A cura di / (Edd.), E. Bani, V. De Stasio, A. Sciarrone Alibrandi, Bergamo, Sestante Edizioni, 2021, pp. 99 a 101;

[94] Artigo 83.º da PRSP. De acordo com o texto introdutório da PRSP, p. 12, esta disposição vem acrescentar clareza ao conceito de "inerência", ao especificar que esses mecanismos de controlo de operações devem basear-se na análise das operações de pagamento, tendo em conta elementos típicos do utilizador de serviços de pagamento nas circunstâncias de uma utilização normal das credenciais de segurança personalizadas.

[95] *Cfr.* Artigo 83.º n.º 2 PRSP. De sublinhar que o prestador de serviços de pagamento apenas poderá conservar esses dados durante o período justificável para o fim a que se destinam, devendo os mesmos serem apagados assim que cesse a relação contratual com o Cliente, *cfr*. texto introdutório da PRSP, p. 12. O Parlamento Europeu, por sua vez, propõe a alteração deste prazo para "*nunca durante mais do que dez anos após a cessação da relação com o cliente*", *cfr.* Resolução legislativa do Parlamento Europeu (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)).

[96] De acordo com Maria Raquel Guimarães, estas características não são inerentes ao utilizador, pelo que a sua eficácia estará dependente da recolha e tratamento de uma grande quantidade de dados, que, em última instância, não podem ser anónimos, sendo que, *"ainda assim, dever-se-á distinguir aquilo que a pessoa é daquilo que é o seu perfil de consumo.*", cit. "«Na minha Conta ou na tua?»…", cit., p. 91.

[97] E em linha com a Diretiva (UE) 2019/882 do Parlamento Europeu e do Conselho 51 relativa aos requisitos de acessibilidade dos produtos e serviços.

[98] Considerando 110 da PRSP.

assegurar que os seus clientes possam beneficiar de diferentes métodos de realização da autenticação forte do cliente, devidamente adaptados às suas necessidades e limitações[99].

3.2.2. Sensibilização e informação sobre fraude

Como vimos referindo, as constantes evoluções tecnológicas possibilitam também um sem número de novos mecanismos de fraude. A diversidade de práticas, nomeadamente, roubo de credenciais de autenticação, adulteração de faturas, ou manipulação social, a acrescer a outras técnicas que vão sendo engendradas ao longo do tempo, conduzem a que o combate a esses novos mecanismos seja, muitas vezes, realizado de forma reativa. É nesta medida que a partilha de informações entre PSPs pode assumir enorme relevância.

É com a finalidade de garantir maior proteção dos utilizadores (consumidores), através da deteção atempada de atividades potencialmente fraudulentas, que a PRSP consagra no artigo 83.º, n.º 4, a possibilidade de os PSPs celebrarem acordos de partilha de informação, devendo ficar definidos, *ab initio,* os termos dessa partilha, nomeadamente, os elementos operacionais e a utilização de plataformas informáticas específicas[100].

A falta de literacia do consumidor em relação ao assunto fraude, é também apontada pela EBA[101], e bem assim, por várias autoridades públicas na consulta específica sobre o tema, questão que veio a ser considerada na PRSP, conforme veremos mais à frente. Assim, no que respeita à promoção de medidas de partilha de conhecimento e de sensibilização dos utilizadores para os riscos e tendências de fraude, este é um ónus que passa também a recair sobre os PSPs, nos termos do artigo 84.º da PRSP. Entendeu o legislador europeu, que os PSPs devem desempenhar um papel essencial na prevenção da fraude, através da promoção de programas educativos e de sensibilização, destinados a aumentar o conhecimento dos clientes quanto a esta matéria, de forma que estejam despertos para situações em que possam ser alvos

---

[99] Artigo 88.º da PRSP. O Parlamento Europeu vai mais longe, e propõe a inclusão de um normativo com a epígrafe "acesso equitativo, razoável e não discriminatório a dispositivos móveis", de acordo com o qual "*os fabricantes de equipamento de origem de dispositivos móveis e os prestadores de serviços de comunicações eletrónicas na aceção do artigo 2.º, ponto 1, da Diretiva (UE) 2018/1972 devem permitir que os prestadores de serviços tenham uma interoperabilidade efetiva e acesso para efeitos de interoperabilidade às características técnicas necessárias para armazenar e transferir dados para realizar operações de pagamento, em condições equitativas, razoáveis e não discriminatórias*", *cfr* artigo88º-A da Resolução legislativa do Parlamento Europeu (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)).

[100] A fim de impor alguma salvaguarda à proteção de dados, os PSP estão obrigados a realizar uma avaliação de impacto conjunta sobre a proteção de dados a que se refere o artigo 35.º do Regulamento (UE) 2016/679 (RGPD) e, se aplicável, consultar previamente a autoridade de controlo, em conformidade com o artigo 36.º desse Regulamento — conforme artigo 83.º, n.º 4 (a final) da PRSP e considerando 103 da PRSP. Do tratamento de dados pessoais partilhados ao abrigo destes acordos de partilha de informação entre PSPs, não deve resultar a cessação da relação contratual que o prestador de serviços de pagamento mantem com o cliente, nem afetar a sua inclusão futura por outro prestador de serviços de pagamento, artigo 83.º, n.º 6 da PRSP.

[101] *Cfr.* recomendação da Autoridade Bancária Europeia (EBA), *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, cit., p. 82.

de possíveis tentativas de fraude[102]. Estes normativos — artigos 83.º e 84.º da PRSP — representam assim uma novidade da PRSP, não encontrando paridade na DSP2. Parece-nos uma iniciativa que irá acrescentar valor no combate à fraude, e consequente proteção dos utilizadores/consumidores.

3.2.3. Serviço de verificação de IBAN

Ainda no âmbito da proteção dos utilizadores, em 26 de outubro de 2022, a Comissão propôs uma alteração do Regulamento SEPA[103], a fim de acelerar e facilitar a utilização de pagamentos imediatos em euros na EU, que resultou na publicação do Regulamento (UE) 2024/886[104], no qual se prevê a obrigação de os prestadores de serviços de pagamento que ofereçam serviços de pagamento que consistam no envio e receção de transferências a crédito, passarem a oferecer também um serviço de pagamento que permita o envio e receção de transferências a crédito imediatas, e bem assim, proporcionarem aos utilizadores um serviço de verificação do IBAN/nome, que mais não é do que a verificação da correspondência entre o identificador único e o nome do beneficiário. Ora, a presente PRSP prevê o alargamento desse requisito de verificação de IBAN/nome aos prestadores de serviços de pagamento que oferecem transferências a crédito em qualquer moeda da UE, com vista a melhorar a qualidade dos serviços prestados e a garantir maior segurança para os utilizadores/consumidores[105].

---

[102] Esta iniciativas podem ser promovidas através de campanhas de sensibilização nos meios de comunicação social ou outros meios de informação direcionados, com finalidade pedagógica, com vista a educar os utilizadores/consumidores para os riscos existentes, assim como, a fornecer as ferramentas necessárias para evitarem possíveis fraudes – *cfr.* considerando 106 da PRSP.

[103] European Commission, *Proposal for a Regulation of the european parliament and of the council amending Regulations, As regards instant credit transfers in euro (EU) No 260/2012 and (EU) 2021/1230*, COM (2022) 546 final 2022/0341 (COD), Brussels, 26.10.2022.

[104] Regulamento (UE) 2024/886 do Parlamento Europeu e do Conselho de 13 de março de 2024, que altera os Regulamentos (UE) n.º 260/2012 e (UE) 2021/1230 e as Diretivas 98/26/CE e (UE) 2015/2366 — as transferências a crédito imediatas, possibilitam que, em qualquer dia e a qualquer hora, e no prazo de 10 segundos a contar do momento da receção da ordem de pagamento, o banco do ordenante disponibilize o montante dessa operação na conta do beneficiário. Os bancos deverão adicionalmente verificar a correspondência entre o IBAN e o nome do beneficiário antes da transação ser efetuada, de modo a alertarem o ordenante de eventuais discrepâncias. Não obstante algumas exceções previstas, os encargos com estas transferências não poderão ser superiores aos aplicáveis às transferências bancárias ditas "normais". A este respeito, vide, José Manuel Navarro Llena*, Del "Pay by Bank" a la PSD3, y viceversa.* de*12-07-2024, disponível em* <Del "Pay by Bank" a la PSD3, y viceversa. | (granadablogs.com)> (18-07-2020).

[105] Esta iniciativa não é totalmente inovadora, tendo já sido adotada nos mercados dos Países Baixos e Reino Unido, onde se revelou altamente eficaz na prevenção de erros e na redução de certos tipos de fraude. No Reino Unido, entre o 3.º trimestre de 2019 e o 4.º trimestre de 2020, numa base ajustada pela tendência, para os maiores PSP que ofereceram o serviço de verificação de IBAN aos clientes, houve uma queda de 31% no número de pagamentos efetuados para um beneficiário errado — Ver: *Payment Systems Regulator, Confirmation of Payee Call for views*, Maio de 2021. Em Portugal este serviço encontra-se disponibilizado desde 20 de maio de 2024, através de duas funcionalidades: a funcionalidade de confirmação de beneficiário singular, que permite confirmar a informação sobre o beneficiário de uma transferência, a crédito ou imediata, devolvendo o nome do primeiro titular da conta de pagamento associada ao IBAN indicado; e a funcionalidade de confirmação de beneficiário/devedor agrupada, que permite confirmar a titularidade de uma ou mais contas de pagamento, através

Em termos práticos, recai sobre o PSP do beneficiário, a pedido do PSP do ordenante, o ónus de verificar a coincidência entre os dados indicados pelo utilizador do serviço de pagamento aquando da ordem de transferência — nome e identificador único do beneficiário (IBAN)[106]. Existindo discrepância entre os dados indicados, o PSP do beneficiário deve notificar o PSP do ordenante desse facto e indicar o grau da discrepância[107]. Esta informação deverá ser prestada imediatamente após o ordenante indicar os dados para a transferência, e antes de lhe ser dada a possibilidade de autorizar a transação; de outro modo, a informação pecaria por tardia. Na eventualidade de o ordenante querer prosseguir com a operação, deverá ser informado sobre as possíveis consequências da sua decisão, nomeadamente, a de se considerar a operação corretamente executada e afastar assim a imputação dos prejuízos decorrentes da transferência, ao PSP.

No caso de o ordenante detetar alguma falha do serviço de verificação de correspondência, da qual resultem operações de pagamento não autorizadas ou incorretamente efetuadas, deverá informar o PSP o mais rapidamente possível, conforme n.º 1 do artigo 54 º da PRSP — dentro de um prazo nunca superior a 13 meses a contar do débito[108]. Verificando-se que houve aplicação incorreta dos serviços de verificação de correspondência[109] (ou não houve aplicação de todo – expetando-se quando a pedido do cliente), o PSP deve, no prazo de 10 dias úteis[110] (a contar da data em que tomou conhecimento), reembolsar o ordenante do montante integral da transferência realizada[111]. Em alternativa, dispõe de igual prazo para

da validação de pares NIF/IBAN ou NIPC/IBAN para transferências a crédito e imediatas e débitos diretos, iniciados de forma agrupada, *cfr.* comunicação do Banco de Portugal, de 20 de maio de 2024.

[106] Artigo 50.º PRSP. Refira-se que a prestação deste serviço é gratuita, no entanto, os utilizadores podem optar por não o receber, *cfr.* artigo 57.º, n. º3.

[107] A este respeito, veja-se o Acórdão do Supremo Tribunal de Justiça de 16-02-2023, (Catarina Serra), proferido à luz do atual regime, segundo o qual, tendo ordenante de uma transferência eletrónica procedido à indicação de determinado IBAN e sendo o pagamento efetuado na conta correspondente a esse IBAN, embora pertencente a pessoa diferente do beneficiário indicado pelo ordenante, não pode este responsabilizar o banco alegando violação do dever de verificar se a pessoa beneficiária correspondia, efetivamente, à indicada na ordem de transferência. Ora, à luz da PRSP, a situação *sub judice* teria enquadramento distinto, na medida em que passa a prever o ónus de o PSP verificar a coincidência entre os dados indicados pelo utilizador do serviço de pagamento aquando da ordem de transferência, devendo, em caso de discrepância, notificar o ordenante, antes deste autorizar a transferência em causa. Veja-se também Maria Raquel Guimarães, "«Na minha Conta ou na tua?»…", cit., pp. 109 a 112.

[108] Memorando 74 da PRSP.

[109] Artigo 57.º da PRSP.

[110] O Parlamento Europeu propõe alteração deste prazo para 14 dias- *cfr.* Resolução legislativa do Parlamento Europeu, (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)), artigo 57.º, n.º 2.

[111] Na eventualidade da falha do serviço de verificação de correspondência ser imputável ao serviço de prestação de pagamentos do beneficiário, o prestador do serviço de pagamento do ordenante terá direito de regresso sobre o mesmo.

apresentar justificação para recusa do reembolso e indicar os organismos para os quais o cliente pode remeter a sua reclamação[112].

Esta responsabilização que recai sobre o PSP, ainda que em caso de fraude, quando os serviços de verificação de correspondência não tenham sido corretamente aplicados, tem em vista incentivar que os PSPs assegurem uma correta e eficaz aplicação deste mecanismo como medida preventiva necessária para combater a fraude, e reflete o caracter imperativo desta norma. Esta medida pretende reforçar a confiança dos clientes no recurso aos pagamentos eletrónicos, ao facilitar a decisão do ordenante em prosseguir com a transação pretendida.

Ainda no âmbito desta temática, é de referir a proposta do Parlamento de alteração à PRSP, no sentido ser acrescentado um normativo de combate à discriminação do identificador de contas de pagamento com base na localização, segundo o qual, no âmbito das transferências a crédito para beneficiários titulares de contas de pagamento situadas na União, não devem os ordenantes ter de especificar o Estado-Membro em que essas contas de pagamento estão localizadas, desde que as mesmas sejam acessíveis. Do mesmo modo, caso os beneficiários aceitem transferências a crédito ou utilizem débitos diretos para a cobrança de fundos junto de ordenantes titulares de contas de pagamento situadas na União, não devem ter de especificar o Estado-Membro em que essas contas de pagamento estão localizadas, desde que, mais uma vez, as mesmas sejam acessíveis[113].

3.3. O *OPEN BANKING*

O *open banking* é um sistema baseado em *fintech*, que permite a partilha de dados e serviços entre instituições bancárias e terceiros, de forma segura e integrada, com o necessário consentimento do cliente[114]. O *open banking*, ou, em português, banca aberta, é assim o mecanismo através do qual os prestadores de serviços de informação sobre contas e os prestadores de serviços de iniciação de pagamento, coletivamente conhecidos como terceiros prestadores de serviços de pagamentos (TPPs), fornecem aos utilizadores de serviços de pagamento um acesso agregado de todos os seus dados financeiros, ainda que, referentes a

[112] Artigo 57.º, n.º 2 da PRSP. Na sua proposta de alteração, o Parlamento acrescenta que a justificação de recusa deve ser apresentada por escrito, assim como, devem ser apresentadas provas à autoridade competente relevante de que não houve lugar à infração do artigo 50.º, n.º 1, isto é, da verificação de correspondência entre o nome e o IBAN do beneficiário, *cfr.* Resolução legislativa do Parlamento Europeu, (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)).

[113] *Cfr*. Resolução legislativa do Parlamento Europeu, (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD))- artigo 50.º-A.

[114] Embora as organizações de consumidores e os consumidores individuais tenham manifestado preocupações com a segurança dos dados no contexto do *open banking*, o *open banking* cresceu na Europa desde a aplicação do PSD2, chegando a quase 19 milhões em 2021–SWD(2023) 231 final, p. 13.

contas geridas por outros prestadores de serviços financeiros[115], bem como, possibilitam aos utilizadores, iniciarem uma ordem de pagamento sem direta interação com o prestador de serviços de pagamento no qual a sua conta está domiciliada.

A Europa contabilizou aproximadamente 12,2 milhões de usuários de *open banking*[116]. A expectativa é que esse número chegue a 63,8 milhões até ao final de 2024[117].

Embora não seja uma inovação da DSP2, esta segunda Diretiva veio estabelecer o quadro regulamentar do *open banking*, de modo a definir as condições em que os PSISC (prestadores de serviços de informação sobre contas) e os PSIP (prestadores de serviços de iniciação de pagamento) podem fornecer os seus serviços, tentando garantir condições equivalentes para o exercício da atividade tanto aos prestadores de serviços de pagamento existentes como aos novos prestadores de serviços de informação sobre contas e prestadores de serviços de iniciação de pagamento[118].

Os serviços de informação sobre contas fornecem informações agregadas dos dados financeiros do utilizador, facilitando o conhecimento e gestão das suas finanças[119]/[120]. Por seu turno, os serviços de iniciação de pagamento, consistem na "emissão de uma ordem de pagamento a pedido do ordenante ou do beneficiário relativamente a uma conta de pagamento detida junto de outro prestador de serviços de pagamento"[121], ou seja, asseguraram ao beneficiário (comerciante *online*) que o pagamento foi iniciado, a fim de incentivar a disponibilização do bem ou a prestação do serviço sem demora indevida[122]. Os PSISCs e os PSIPs apresentam-se assim como uma terceira parte facilitadora entre prestadores de serviços de pagamento e os utilizadores/consumidores.

---

[115] *Vide* considerando 54 da PRSP. Também conforme Francisco Mendes Correia, "Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento", cit., p. 395.

[116] Statista Research Department, *Open banking users worldwide in 2020 with forecasts to 2024, by region*, de 17-05-2023, disponível em < Open banking users worldwide by region | Statista> (26-05-2024).

[117] Idem. À escala mundial, em 2020, 4,7 milhões de pessoas físicas usavam serviços de open banking, número que deve chegar a 132,2 milhões de utilizadores até ao final de 2024.

[118] Sobre o tema, Francisco Mendes Correia, "Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento", cit., p. 388.

[119] Artigo 3.º, n.º 21 da PRSP e artigo 4.º, n.º 16 da DSP2; considerando 54 da PRSP. Ver também, Francisco Mendes Correia, "Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento", cit., p. 397.

[120] Os PSISCs requerem o consentimento do "usuário do serviço de pagamento" para aceder aos dados junto dos prestadores de serviços de pagamento, sendo que, o acesso, armazenamento e uso desses dados, é limitado ao necessário para executar o serviço explicitamente consentido pelo utilizador- artigo 47.º, n.º 1 da PRSP e artigo 67.º, n.º 2 DSP2.

[121] Artigo 3.º, n.º 20 da PRSP e artigo 4.º, n.º 15 da DSP2.

[122] Neste sentido o considerando 29 da DSP2, bem como, considerando 54 da PRSP. Ver também, Francisco Mendes Correia, "Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento", cit., p. 396.

A DSP2 parece ter tido sucesso no que respeita à garantia da segurança na partilha de dados dos usuários no âmbito do *open banking*[123]; no entanto, a regulamentação geral do *open banking* terá ficado aquém do expectável[124], nomeadamente, no que respeita ao acesso dos TPPs às contas de pagamento dos utilizadores[125]. Por outro lado, a ineficiência do *open banking* está também relacionada com a falta de pormenor e clareza do quadro jurídico, nomeadamente, no que respeita ao nível de desempenho esperados pelas API (*application programming interface)*[126], e bem assim, à natureza dos dados e funcionalidades a disponibilizar. A escassa concretização legislativa quanto a esta matéria, abriu portas a que alguns "terceiros" prestadores de serviços de pagamento, atuando como "agregadores de informação", repassassem dados dos PSU (*payment service user*) para quartas-partes não regulamentadas[127]. Embora a obtenção de dados seja efetuada com o consentimento dos utilizadores dos serviços de pagamento, em conformidade com as normas do RGPD, esta atividade não se encontra regulamentada no âmbito da DSP2; porém, também não é clara a sua exclusão[128]

Assim, não obstante os esforços de clarificação desenvolvidos pós DSP2[129], os mesmos não se revelaram suficientes, continuando a subsistir uma grande incerteza no mercado, e entre as autoridades de supervisão, quanto ao que constitui um *obstáculo proibido* aos serviços de banca aberta regulamentados, pelo que, o *open banking* continua a funcionar de forma imperfeita.

---

[123] É pelo menos isto que resulta da avaliação efetuada ao desempenho da DSP2- *vide*, SWD(2023) 231 final; ANNEX 2: Stakeholder consultation.

[124] Idem. Também neste sentido o texto introdutório da PRSP, p. 15.

[125] Problema já identificado antes da entrada em vigor da DSP2, conforme Francisco Mendes Correia, "Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento", cit. p. 398. De acordo com o considerando 67 da PRSP, a revisão da Diretiva (UE) 2015/2366 revelou que os prestadores de serviços de informação sobre contas e de iniciação de pagamentos continuam a estar expostos a muitos obstáculos injustificados, apesar da proibição desses obstáculos imposta pelo artigo 32.º, n.º 3, do Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de novembro de 2017, que complementa a DSP2 no que respeita às normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras.

[126] A respeito desta temática, *vide* o parecer emitido pela Autoridade Bancária Europeia (EBA), *Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC*, (EBA/OP/2020/10), 4 de junho de 2020, disponível em <EBA Opinion on obstacles under Art. 32(3) RTS on SCA&CSC.pdf (europa.eu)> (26-05-2024).

[127] SWD(2023) 231 final, p. 15. É apontado o exemplo dos credores que desejam avaliar a solvabilidade dos devedores, e que têm assim interesse na obtenção dos dados financeiros dos mesmos.

[128] Idem; Autoridade Bancária Europeia (EBA), *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, cit., ponto 23; e ainda, Q&A da EBA, *Clarification on whether a particular business model type constitutes the provision of an account information service as defined by Article 4 (16) of PSD2*, Q&A 2018_4098, de 13 de setembro de 2019, disponível em: <2018_4098 Clarification on whether a particular business model type constitutes the provision of an account information service as defined by Article 4 (16) of PSD2 | European Banking Authority (europa.eu)> (26-05-2024).

[129] A EBA teve oportunidade a analisar todas estes "entraves" no seu parecer de junho de 2020, *intitulado Obstacles to the provision of third-party provider services under the Payment Services Directive*

A PRSP começa desde logo por prever, nos termos do artigo 33.º, n.º 1, que "os prestadores dos serviços de pagamento não podem impedir os utilizadores dos serviços de pagamento de recorrer a um prestador de serviços de iniciação de pagamento" [130]. No mesmo sentido, refere o n.º 2, do artigo 33.º que os prestadores dos serviços de pagamento "não podem impedir os utilizadores de serviços de pagamento de utilizar serviços de informação sobre contas". Ora, estes preceitos traduzem a clara imposição do *open banking* aos prestadores de serviços de pagamentos[131].

Por outro lado, a PRSP vem estabelecer a possibilidade de os prestadores de serviços de pagamento fixarem taxas pela disponibilização dos dados no âmbito da banca aberta, o que poderá incentivar a uma maior cooperação e investimento na inovação por parte dos prestadores de serviços de pagamento. Ao abrigo do enquadramento fornecido pela DSP2, o acesso aos dados por parte dos PSICs e PSIPs tem sido efetuado sem uma base contratual, e nesta medida, sem a possibilidade de cobrança de encargos[132]. Não obstante as vantagens que se adivinham, o legislador optou por não consagrar esta imposição contratual, concedendo apenas essa possibilidade ao livre-arbítrio das entidades em causa[133]/[134].

Conforme já mencionado, outra questão que tem obstado à implementação plena da banca aberta, tem sido a falta de clarificação quanto à *interface* a utilizar por parte dos prestadores de serviços de iniciação de pagamentos e prestadores de serviços de informação

[130] O artigo 66.º, n.º 1 da DSP2 dispõe em sentido semelhante, "*Os Estados-Membros asseguram que o ordenante tenha direito a recorrer a um prestador do serviço de iniciação do pagamento (...)".* Não obstante a semelhança entre ambos os normativos, no âmbito da PRSP o legislador quis ir mais longe, referindo expressamente o facto de os prestadores de serviços de pagamento não poderem impedir o acesso do utilizador a um prestador de serviço de iniciação de pagamentos; no mesmo sentido no que se refere aos serviços de informação sobre contas.

[131] Em relação a esta temática, cumpre referir as alterações propostas pelo Parlamento Europeu, no sentido de os beneficiários deverem oferecer aos utilizadores pelo menos um método de pagamento livre de encargos suplementares e que não dependa do recurso a um prestador de serviços de iniciação de pagamentos, bem como, os comerciantes, como os credores e os operadores de seguros deverem oferecer aos utilizadores de serviços de pagamento uma forma de partilharem os seus dados que não dependa do recurso a prestadores de serviços de informação sobre contas, acrescentando ainda, sem prejuízo do Regulamento (UE) 2016/679, o dever de os PSPs informarem os consumidores de forma clara e compreensível, sempre que lhes seja apresentada uma oferta personalizada baseada no tratamento automatizado de dados pessoais, *cfr.* art.33.º 1-A., 2-A e 2-B.da Resolução legislativa do Parlamento Europeu, (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD).

[132] Já neste sentido, Francisco Mendes Correia, "Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento", p. 399.

[133] O legislador justifica a manutenção do quadro em vigor, sem relação contratual e, por conseguinte, sem cobrança de encargos, uma vez que entende que, se os serviços regulamentados de acesso aos dados fossem sujeitos a encargos, o impacto sobre a continuação da prestação desses serviços, bem como, sobre a concorrência e a inovação nos mercados de pagamentos, poderia ser muito significativo em termos negativos, conforme considerando 55 da RPSP.

[134] Artigo 34.º, n.º 1 e 2 da PRSP. Os prestadores de serviços de pagamento que gerem contas e os prestadores de serviços de informação sobre contas e de iniciação de pagamentos podem estabelecer uma relação contratual, nomeadamente no contexto de um acordo contratual multilateral, prevendo uma eventual compensação pelo acesso aos dados das contas de pagamento e pela prestação de serviços de banca aberta. Considerando 56 da PRSP.

sobre contas[135]. A DSP2 oferece pouca clareza no que respeita a esta temática, e nesse sentido, tem sido motivo de querela entre os prestadores de serviços de pagamento gestores de contas e os prestadores de serviços de iniciação de pagamentos e prestadores de serviços de informação sobre contas. A PRSP vem assim tratar este tema com maior pormenor, em busca de maior clarificação das "regas do jogo" para os diferentes intervenientes, de forma a potencializar o recurso ao *open banking*, começando por determinar que os PSPs que gerem contas devem dispor de uma *interface* específica concebida para a partilha de dados com os PSICs e PSIPs, dispensando-os de manter em permanência outras *interface*s de recurso[136]. Assim, salvo situações em que estas *interface*s se encontrem inoperacionais, os PSICs e PSIPs devem abster-se de utilizar a *interface* do cliente do prestador de serviços de pagamentos que gere contas, situação que tem sido bastante recorrente ao abrigo da DSP2, e que tem sido alvo de manifesto descontentamento por parte dos PSPs que gerem contas, conforme já tivemos oportunidade de referir. O recurso a outra *interface* (direta), por parte dos PSICs e PSIPs, só poderá ter lugar em situações excecionais, perante a falha da *interface* específica, com vista a assegurar que estes possam continuar a sua atividade, sem interrupções inesperadas e geradoras de graves prejuízos[137]. Assim, perante a indisponibilidade da *interface*, os PSICs e PSIPs poderão, mediante pedido dirigido à autoridade competente para o efeito, socorrer-se da *interface* que o PSP que gere contas disponibiliza diretamente para o seu cliente para acesso a dados de contas e pagamento[138]. O legislador clarifica assim o recurso à *interface* que o prestador de serviços de pagamentos que gere contas utiliza para a autenticação e comunicação com os seus

[135] A este respeito, ver Toni Berga, "*Del 'open banking' de PSD2 al 'open finance' de PSD3*", de 01-02-2023, disponível em <Del 'open banking' de PSD2 al 'open finance' de PSD3 | Embat> (04-06-2024).
[136] Artigo 35.º, n.º 1 e 2 da PRSP e Considerando 57 da PRSP.
[137] Artigo 38.º, n.º 2 da PRSP e considerando 60 da PRSP. Nesta medida, os prestadores de serviços de pagamentos gestores de contas devem informar os prestadores de serviços de informação sobre contas e prestadores de serviços de iniciação de pagamentos das medidas tomadas para restabelecer a *interface* e do tempo estimado para o efeito.
[138] De acordo com o considerando 60, a autorização de acesso aos dados que necessitam para assegurar a continuidade das suas atividades será extensível a todos os prestadores de serviços de informação sobre contas e de iniciação de pagamentos, e não apenas aqueles que apresentaram o pedido; neste sentido, o artigo38º, n.º 3 e 4 da PRSP. Nota especial para o facto de, como medida de salvaguarda dos prestadores de serviços de informação sobre contas e prestadores de serviços de iniciação de pagamentos, o legislador consagrar que, enquanto a autoridade competente não tomar uma decisão sobre o pedido apresentado, "*o prestador se serviços de iniciação de pagamentos ou o prestador de serviços de informação sobre contas requerente pode aceder, a título excecional, aos dados das contas de pagamento através de uma interface que o prestador de serviços de pagamentos que gere contas utiliza para a autenticação e comunicação com os seus utilizadores*"- artigo 38.º, n.º 4 da PRSP. No considerando 61 o legislador alerta, no entanto, para a cautela necessária, sendo que esse acesso direto temporário não deve ter efeitos negativos para os consumidores. Os prestadores de serviços de informação sobre contas e de iniciação de pagamentos devem sempre identificar-se e respeitar todas as suas obrigações, designadamente, os limites da autorização que lhes foi concedida, devendo aceder apenas aos dados que necessitam para prestar os serviços contratualizados. A nova proposta de Regulamento prevê ainda que a autoridade competente deve estabelecer prazos para que o prestador de serviços de pagamento que gere contas reestabeleça em pleno o funcionamento da *interface* específica, sob pena de serem aplicadas sanções em caso de incumprimento, *cfr.* considerando 60 de PRSP.

utilizadores, como medida excecional, de modo a colmatar as diferentes interpretações retiradas da DSP2 e os diferendos gerados entres os diferentes prestadores de serviços de pagamento, sem, no entanto, deixar de assegurar a continuidade da atividade prestada pelos PSICs e PSIPs.

Com vista a colocar cobro à discrepância (e escassez) de dados e funcionalidades fornecidos, a proposta de Regulamento vem agora elencar os requisitos de segurança e desempenho[139], e bem assim, as funcionalidades mínimas[140], das *interface*s específicas de acesso aos dados fornecidos pelos prestadores de serviços de pagamentos que gerem contas[141]. No que respeita aos prestadores de serviços de iniciação de pagamentos em concreto[142], o prestador de serviços de pagamento que gere a contas fica obrigado a fornecer todas as informações a que tenha acesso relativas à execução da operação de pagamento logo após a receção da ordem de pagamento[143], inclusive, as informações suplementares de que tenha conhecimento após a ordem de pagamento e antes da execução do mesmo. Esta questão assume especial importância no que respeita à segurança e proteção dos utilizadores, sendo fundamental garantir que o prestador de serviços de iniciação de pagamento tem acesso a todas as informações relevantes, de forma a que possa avaliar o risco envolvido na operação em causa[144].

Esta concretização visa conferir, mais uma vez, clareza e definição ao quadro normativo dos serviços de pagamento, na expectativa de colocar termo (ou, pelo menos, reduzir significativamente) aos litígios entre os PSPs que gerem contas e os prestadores de serviços de iniciação de pagamentos ou prestadores de serviços de informação sobre contas. Esta é mais uma alteração que carece de ser saudada, uma vez que, com a definição dos requisitos mínimos, não será concedido espaço a *interface*s ineficientes e com escassez de conteúdo.

Não obstante, legislador não se mostrou indiferente ao ónus desproporcional que pode representar para alguns prestadores de serviços de pagamento que gerem contas a

---

[139] Artigo 36.º, n.º 1da PRSP.
[140] O artigo 36.º, n.º 2 elenca as funcionalidades mínimas da *interface* específica a ser disponibilizada pelo PSP aos prestadores de serviços de iniciação de pagamento e prestadores de serviço de informação sobre conta.
[141] O legislador refere no Considerando 59 que a *interface* a disponibilizar deve assegurar no mínio "*paridade de dados com a interface do cliente disponibilizada aos seus utilizadores pelo prestador de serviços de pagamento que gere a conta*", incluindo, dados da conta de pagamento. No que diz respeito aos serviços de iniciação de pagamentos, a *interface* específica deve permitir, não só a iniciação de pagamentos de caráter isolado, como a possibilidade de promover ordens permanentes e débitos diretos. O legislador prevê ainda que que devem ser estabelecidos requisitos mais pormenorizados para as *interface*s específicas, nas normas técnicas de regulamentação a serem elaboradas pela EBA; neste sentido, o artigo37.º da PRSP.
[142] Artigo 36.º, n.º 4 elenca as funcionalidades mínimas da *interface* específica a ser disponibilizada pelo PSP especificamente aos prestadores de serviços de iniciação de pagamento.
[143] Artigo 40.º, alínea b) da PRSP.
[144] Memorando 64 da PRSP.

disponibilização de interfaces específicas, possibilitando a dispensa de uma interface específica, ou, em alternativa, a disponibilização do acesso à interface que o PSP utiliza para autenticação e comunicação com os utilizadores dos serviços de pagamento, mediante pedido dirigido à autoridade competente [145].

Por outro lado, o serviço de *open banking* reclama, também, por garantias de proteção dos utilizadores. Os utilizadores dos serviços de informação sobre contas ou de iniciação de pagamentos devem ter total controlo sobre os seus dados que possam vir a ser partilhados, e ter acesso às autorizações de acesso aos dados eventualmente concedidas aos prestadores de serviços de pagamentos[146], devendo ser disponibilizados mecanismos/ferramentas de controlo que permitam gerir (conceder, revogar e modificar) as autorizações concedidas aos prestadores de serviços de banca aberta[147].

Outra temática relevante prende-se com a gestão de dados efetuada pelos prestadores de serviços de informação sobre contas. A revisão da Comissão fez referência ao facto de os prestadores de serviços de informação sobre contas autorizados fornecerem, por vezes, dados relativos a contas de pagamento que agregam, a entidades terceiras, com a finalidade de lhes permitirem prestar outros serviços aos utilizadores[148]. A questão reside em esclarecer se esta atividade deve, ou não, considerar-se abrangida pelo serviço regulamentado de informação sobre contas. De acordo com o considerando 26 da PRSP, a Comissão considera que "esta evolução da «licença como serviço» do modelo de negócio de «banca aberta» pode ser uma fonte de serviços inovadores e baseados em dados", com benefício direto para os

[145] Artigo 39.º da PRSP. No termos do artigo 37.º da PRSP, o legislador europeu consagra também desta feita a equidade de acesso aos dados entre a *interface* específica e a *interface* do cliente, cuidando de garantir que o utilizador que recorra a um prestador de serviços de informação sobre contas, disponha da mesma informação a que teria acesso através da *interface* direta do seu prestador de serviços de pagamentos que gere a conta. Do mesmo modo, quando o utilizador recorre aos serviços de um prestador de serviços de iniciação de pagamento, devem ser facultadas, pelo menos, as mesmas informações sobre a iniciação e execução da operação de pagamento que seriam facultadas se tivesse recorrido ao seu prestador de serviços de pagamento gestor de conta. O legislador vem assim, uma vez mais, concretizar os dados que devem, imperativamente, ser facultados pelo prestador de serviços de pagamento que gere a conta, através da interface específica, possibilitando que os prestadores de serviços de iniciação de pagamentos ou o prestador de serviços de informação sobre contas sejam capazes de prestar um serviço de alta qualidade aos seus clientes.

[146] Considerando 65 da PRSP.

[147] O preâmbulo da PRSP fala em "*painel de controlo*". De acordo com ortigo 43.º o n.º 2 da PRSP, esse painel de controlo deve facultar ao utilizador de serviços de pagamento uma visão geral de cada autorização em curso concedida para efeitos de serviços de informação sobre contas ou de serviços de iniciação de pagamentos, incluindo, permitir que o utilizador de serviços de pagamento retire o acesso aos dados de um determinado prestador de serviços de informação sobre contas ou de serviços de iniciação de pagamentos; permitir que o utilizador de serviços de pagamento restabeleça qualquer acesso aos dados retirado; e bem assim, incluir um registo das autorizações de acesso aos dados que tenham sido retiradas ou que tenham caducado por um período de dois anos. A respeito deste tema, é de salientar ainda que o tratamento dos dados pessoais deverá sempre respeitar o RGPD e o Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, incluindo os princípios da limitação das finalidades, da minimização dos dados e da limitação dos prazos de conservação.

[148] Considerando 26 da PRSP.

utilizadores[149]. Nestes termos, caberá ao utilizador definir o limite de acesso aos seus dados, devendo este ter total conhecimento de quem acede aos dados das suas contas, com que fundamentos jurídicos e com que finalidade, de forma a conceder, ou não, o referido acesso[150].

Face à análise cuidada do quadro normativo apresentado na proposta de Regulamento dos serviços de pagamento, concluímos que o legislador traça um caminho que tem em vista aproveitar o pleno potencial da banca aberta na UE, estabelecendo um regime que visa colmatar o tratamento discriminatório dos prestadores de serviços de informação sobre contas e dos prestadores de serviços de iniciação de pagamentos, fomentando a equidade de condições, face aos prestadores de serviços de pagamentos bancários.

É de ressalvar que o *open banking* foi tema que mereceu especial atenção por parte do legislador, tendo sido dedicado um inteiro capítulo no âmbito da PRSP, em contraponto com a DSP2, que regulamenta os prestadores de serviços de iniciação de pagamento e os prestadores de serviços de informação sobre contas em dois normativos apenas[151]. O legislador procura maior harmonização, com a definição de critérios mínimos, de modo a suprimir diferentes interpretações e extensões das *interface*s específicas disponibilizadas pelos prestadores de serviços de pagamentos que gerem contas. Em suma, o quadro normativo relativo à banca aberta consagrado na PRSP contém uma série de alterações, e passou a incorporar algumas disposições atualmente previstas numa norma técnica de regulamentação[152]. Entendemos que com este novo quadro regulamentar serão derrubados muitos dos obstáculos aos quais estavam expostos os prestadores de serviços de banca aberta.

---

[149] No termos do considerando 26 da PRSP, esta partilha de dados permite que os utilizadores possam ter acesso a outro tipo de serviços não relacionados com pagamentos, incluindo empréstimos, contabilidade e avaliação da solvabilidade. Este entendimento merece, porém, a nossa crítica. Somos da opinião de que os dados agregados no âmbito dos serviços de informação sobre contas deverão ser direcionados exclusivamente para uso do utilizador, não parecendo razoável que os mesmos sejam partilhados com terceiros, não obstante os benefícios elencados. Na nossa ótica esta partilha com entidades terceiras, será geradora de maior risco e menor proteção para os utilizadores, colidindo com os princípios de proteção de dados do RGPD. A este respeito, saudamos a proposta do Parlamento, no sentido de incluir no "painel de controlo" a possibilidade de permitir que os utilizadores de serviços de pagamento se autoexcluam em termos gerais da partilha de dados com terceiros, no que diz respeito a todos os pedidos presentes e futuros de autorização de acesso a dados, *cfr*. consta na Resolução legislativa do Parlamento Europeu (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)), artigo 43.º, n.º 2 c-A).

[150] A fim de proporcionar a proteção adequada aos dados das contas de pagamento dos utilizadores, o serviço de agregação de dados a partir de contas de pagamento deve ser sempre prestado por uma entidade regulamentada com base numa licença, mesmo que os dados sejam, em última análise, transmitidos a outro prestador de serviços. A este respeito, propõe o Parlamento Europeu, que a EBA, em consulta com o Comité Europeu para a Proteção de Dados, deve elaborar orientações sobre a aplicação do artigo 37.º da PRSP, no que se refere aos serviços de iniciação de pagamentos e aos serviços de informação sobre contas, em conformidade com o artigo 16.º do Regulamento (UE) n.º 1093/2010- Resolução legislativa (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)).

[151] Artigo 66.º e 67.º da DSP2, já mencionados anteriormente.

[152] Regulamento Delegado (UE) 2018/389 da Comissão no que diz respeito às normas técnicas de regulamentação para uma autenticação forte do cliente e a normas abertas de comunicação comuns e seguras.

Por fim, é de salientar o papel preponderante que as autoridades nacionais competentes deverão assumir neste desafio[153]. O sucesso da banca aberta reclama por uma rigorosa e eficaz aplicação das regras que regem a atividade, sob pena de o quadro regulamentar previsto se revelar inócuo. Para o efeito, terão de contribuir as autoridades nacionais competentes, que devem dispor de recursos adequados para garantirem o estrito cumprimento das normas relativas ao *open banking*, nomeadamente, através de fiscalização da atividade dos prestadores de serviços de pagamento e consequente aplicação de sanções quando detetem algum incumprimento.

3.4. O ACESSO AOS SISTEMAS DE PAGAMENTO E A CONTAS BANCÁRIAS POR PARTE DOS PSP NÃO BANCÁRIOS

Da avaliação realizada da DSP2, resultaram também limites que têm obstado a condições de concorrência equitativas resultantes do contínuo desequilíbrio entre prestadores de serviços de pagamento bancários e não bancários[154], nomeadamente, pelos obstáculos enfrentados por estes últimos no acesso direto a sistemas de pagamento e a contas bancárias, essenciais para prossecução da sua atividade[155].

Nos termos do artigo 36.º da DSP2, os bancos estão obrigados a notificar as autoridades competentes, por escrito e com a devida justificação, sempre que recusem conceder aos PSPs não bancários a abertura de uma conta. No entanto, esta salvaguarda não está prevista para os casos em que, posteriormente, os bancos decidem encerrar essas contas, o que resulta na necessária interrupção do serviço prestado pelo PSP não bancário, até que seja encontrada uma nova instituição de crédito para abertura de conta[156]. Esta "migração" para a alçada de outro prestador de serviço de pagamento bancário, para além de geradora e enorme insegurança, é também bastante onerosa para os PSPs em questão[157].

Na proposta de Regulamento transparecem os esforços do legislador em dar resposta a estas problemáticas, que têm sido geradoras de perturbações na atividade dos prestadores de serviços de pagamentos não bancários, que veem a sua posição fragilizada ao dependerem

---

[153] As funções das autoridades competentes encontram-se consagradas no artigo 48.º da PRSP.
[154] Sobre este tema, Camden Fine, "Digitalización financiera: el community banking en la era de la disrupción digital", *in Transformación digital y medios de pagouna visión práctica a la luz de la PSD2*, coordinado por Santiago Carbó y Francisco Rodríguez Fernández, Papeles de economía española, N.º 149, 2016. ISSN: 0210-9107, Madrid, p 18.
[155] Preâmbulo da PRSP, p. 4.
[156] Autoridade Bancária Europeia (EBA), *Opinion of the European Banking Authority on "de-risking"*, (EBA/Op/2022/01) 5 de janeiro de 2022, p. 11, disponível em <EBA Opinion and annexed report on de-risking.pdf (europa.eu)>(26-05-2024).
[157] Neste sentido o texto introdutório da PRSP, p. 6.

diretamente da "boa vontade" dos operadores de serviços de pagamentos, para o exercício da sua atividade.

A DSP2 espelha já a preocupação do legislador em assegurar o acesso aos serviços de contas de pagamento junto das instituições de crédito, por parte dos prestadores dos PSPs não bancários, "numa base objetiva, não discriminatória e proporcionada"[158]. Ora, na proposta de Regulamento agora apresentada, o legislador vem concretizar com maior rigor o regime existente, optando por "excecionar", isto é, elencar desde logo as concretas situações em que as intuições de crédito podem recusar a abertura de conta a uma instituição de pagamento ou encerrá-la[159]. Com vista a garantir coerência e transparência almejada pelo legislador, a decisão de recusa ou de encerramento de uma conta deverá sempre ser notificada à instituição de pagamento requerente[160]. Ou seja, recai sobre as instituições de crédito o ónus de apresentar o motivo de rejeição de abertura, ou de decisão encerramento, de uma conta[161].

A PRSP vem também reforçar a posição dos serviços de pagamentos não bancários através da clarificação das regras de acesso aos sistemas de pagamentos[162]. À semelhança da DSP2[163], a PRSP prevê que os PSPs bancários devem dispor de regras objetivas, não discriminatórias, transparentes e proporcionais de acesso a um sistema de pagamento por parte

[158] Artigo 36.º da DSP2.

[159] De acordo com o artigo 32.º, n.º 1, da PRSP, são fundamentos de recusa ou de encerramento, os seguintes casos: quando tenham motivos sérios para suspeitar da existência de controlos deficientes de branqueamento de capitais ou de financiamento de terrorismo; exista ou tenha existido violação de um contrato por parte da instituição de pagamento; não tenham sido fornecidas as informações e documentos necessários para abertura ou manutenção da conta; perfil de risco excessivo; ou, de alguma forma, representar um custo de conformidade desproporcionalmente elevado para a instituição de crédito. É de referir a proposta de alteração apresentada pelo Parlamento- Resolução legislativa do Parlamento Europeu (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)) — , que pretende reforçar este normativo no que respeita à salvaguarda da posição dos PSPs não bancários, nomeadamente, através da imposição de um prazo de pré-aviso, nunca inferior a quatro meses, para que produza efeitos o efetivo encerramento da conta de pagamento, salvo se a conta for encerrada por motivos relacionados com fraude ou atividades ilegais.

[160] De forma fundamentada, concretizando os motivos da recusa, que deverão ter por base os riscos inerentes à atividade ou o cariz da atividade planeada- artigo 32.º, n.º 3, da PRSP. Na proposta de alteração apresentada pelo Parlamento, acrescenta-se que, a instituição de crédito deve ainda notificar a autoridade nacional competente da sua decisão de recusa, bem como, promover a publicação dos dados agregados sobre as recusas de abertura e os encerramentos de conta.

[161] A este respeito, com vista a harmonizar e a garantir maior coerência, recai sobre a EBA o dever de elaborar normas técnicas de regulamentação que especifiquem o formato e as informações e a fundamentação a contemplar nas notificações a remeter para as intuições de pagamento — artigo 31.º, n.º 5, da PRSP. Mais uma vez, o legislador assegura a possibilidade de recurso a uma entidade competente, por parte das instituições de pagamento, perante uma decisão de recusa de acesso a uma conta ou uma decisão de encerramento de conta, a esperança de que seja um mecanismo dissuasor de comportamentos abusivo por parte das intuições de créditos- artigo 31.º, n.º 4, da PRSP. O Parlamento propõe ainda uma alteração ao n.º. 5 do artigo 32.º da PRSP, no sentido de a EBA dever concretizar os motivos objetivos, não discriminatórios e proporcionados e as situações em que uma instituição de crédito pode recusar abrir ou encerrar uma conta de pagamento a uma instituição de pagamento, aos seus agentes ou distribuidores ou a um requerente de uma licença como instituição de pagamento — Resolução legislativa do Parlamento Europeu (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)).

[162] Considerando 31 da PRSP e artigo 31.º da PRSP.

[163] Artigo 35.º, n.º 1, da DSP2.

de prestadores de serviços de pagamento (não bancários) autorizados ou registados para o efeito. A inibição do acesso a um sistema de pagamentos só poderá ocorrer na estrita medida do necessário para acautelar riscos específicos[164]. Mais uma vez, a letra da lei passa por um conceito amplo, sendo que a dificuldade reside em compreender de que forma o quadro regulamentar da PRSP pretende acautelar o princípio de "não discriminação". Ao comparamos o regime consagrado na DSP2 e o regime proposto para o novo Regulamento dos serviços de pagamento, verificamos que, não obstante as semelhanças entre ambos, desta feita, o legislador europeu procurou maior concretização, de forma a limitar os entraves que possam conduzir à inibição de acesso a um sistema de pagamentos. Neste sentido, o n.º 2 do artigo 31.º da PRSP estipula que os operadores de sistemas de pagamentos disponibilizem *ab initio* os critérios de admissão à participação nos seus sistemas de pagamento, bem como, os parâmetros e a metodologia utilizada para avaliação dos riscos dos requerentes de participação[165]. Após a receção de um pedido de acesso ao seu sistema de pagamentos, e posterior avaliação dos riscos inerentes, o operador do sistema de pagamentos deve comunicar, por escrito, ao prestador de serviços de pagamento, a sua decisão de deferimento ou de recusa, sendo que, em caso de recusa, a mesma deverá ser devidamente fundamentada[166].

O legislador procurou estabelecer um quadro regulamentar claro e transparente, com menor discricionariedade para os operadores de sistemas de pagamentos bancários no que concerne à recusa de acesso aos sistemas de pagamento, com vista a trazer maior estabilidade para esta atividade. Ao mesmo tempo, não são descuradas as questões de segurança, mantendo-se um controlo cauteloso no acesso aos sistemas de pagamentos, com crivo apertado no que concerne à avaliação dos perfis dos prestadores de serviços de pagamentos e aos riscos que os mesmos possam abarcar para um sistema de pagamentos[167].

---

[164] *Cfr*. artigo 31.º, n.º 1 da PRSP. No que concerne à supervisão do estrito cumprimento do aqui estipulado, nos casos em que o sistema de pagamentos em questão já esteja sujeito a supervisão pelo Sistema Europeu de Bancos Centrais nos termos do Regulamento (UE) n.º 795/201442 do Banco Central Europeu, o banco central ou os bancos exercem essa supervisão, devendo vigiar o respeito por essas regras no âmbito das suas funções de supervisão. No caso de outros sistemas de pagamento, os Estados-Membros deverão designar autoridades nacionais competentes para assegurar que os operadores de infraestruturas de sistemas de pagamento respeitem esses requisitos, *cfr.* Considerando 32 da PRSP.

[165] Os requisitos que venham a ser fixados pelos operadores de sistemas de pagamentos não podem contemplar regras que de alguma forma restrinjam o recurso dos prestadores de serviços de pagamento a outros sistemas de pagamentos, bem como, regras que façam discriminação entre prestadores de serviços autorizados ou registados, e bem assim, quaisquer restrições relacionadas com a forma social, conforme artigo 31.º, n.º 5 da PRSP.

[166] Isto é, tendo em consideração as regras e procedimentos de admissão, bem como, os critério e metodologia fixados para avaliação do risco inerente, em caso de recusa de acesso ao seu sistema, o operador de sistema de pagamentos deverá concretizar em que medida o prestador de serviços de pagamentos não responde a esses critérios previamente fixados – considerando 31 da PRSP.

[167] Como vimos referindo, de nada serve um quadro regulamentar adequado, se não existirem garantias da sua concreta aplicação. Nestes termos, o legislador europeu mostrou estar consciente dessa necessidade, prevendo a necessidade de criação de uma autoridade de "recurso", que zele pela aplicação das regras estabelecidas no âmbito

Assim, em jeito de conclusão, cumpre referir que, também nestas matérias o legislador vem propor algumas novidades face ao quadro da DSP2, que não representam alterações estruturais, antes sim, o reforço da execução das regras já definidas no âmbito da DSP2, mas que aparentam acarretar maior segurança e estabilidade no que concerne à regulamentação dos serviços de pagamento, e por isso, são dignas de total aprovação, na esperança de que se revelem capazes de colmatar as entropias a que alguns prestadores de serviços de pagamentos estão expostos no âmbito da sua atividade.

4. OPERAÇÕES DE PAGAMENTO

Conforme refere Francisco Mendes Correia, os serviços de pagamento são tratados como atividades em abstrato, que depois são concretizadas em operações de pagamento[168].

Ora, de acordo com o artigo 3.º, n.º 5, da PRSP[169] uma operação de pagamento consiste num ato, iniciado pelo ordenante, ou em seu nome, ou pelo beneficiário, de depositar, transferir ou levantar fundos, independentemente de quaisquer obrigações subjacentes entre o ordenante e o beneficiário. Estas operações de pagamento podem ocorrer isoladamente ou vir enquadradas no âmbito de um contrato-quadro. Têm assim subjacente um contrato bancário.

Cumpre começar por fazer uma breve imersão no conceito de contrato bancário, que, conforme refere Miguel Pestana Vasconcelos, não sendo legalmente típico é "socialmente típico, tendo em conta, de entre outros aspetos, a uniformidade das cláusulas contratuais gerais a que os diversos bancos recorrem"[170], podendo ser definido como "o acordo havido entre uma instituição bancária e um cliente «através do qual se constitui, disciplina e baliza a respetiva relação jurídica bancária»"[171]. Consiste num "contrato organizatório, complexo, com produção de efeitos imediatos, direitos e obrigações para as partes, correspondentes a tipos de prestação de serviços"[172]. Nos termos do n.º 25 do artigo 3.º da PRSP, o contrato-quadro é definido como um contrato de serviços de pagamento que rege a execução futura de operações de pagamento

da PRSP no que respeita ao acesso aos sistemas de pagamentos, garantindo, nomeadamente, a possibilidade de os prestadores de serviços de pagamento recorrerem a uma autoridade competente, que deve ser designada pelos Estados-Membros, em caso de recusa (injustificada) de acesso a um sistema de pagamento, *cfr.* n.º 7 do artigo 31.º da PRPS.

[168] Francisco Mendes Correia, em "Operações não autorizadas e o Regime jurídico dos serviços de pagamento e da moeda eletrónica", *Revista de Direito Civil*, Ano II (2017), Número 3, Coimbra, Almedina, 2017; 701-72, p. 704.

[169] Correspondente ao artigo 4.º, n.º 5 da DSP2.

[170] *Cfr*. Miguel Pestana Vasconcelos, em "A responsabilidade do banco por operações de pagamento não autorizadas no online banking…", cit., p. 192.

[171] José Engrácia Antunes, *Direito dos Contratos Comerciais*, Almedina, 2009, cit. p. 483.

[172] Miguel Pestana Vasconcelos, em "A responsabilidade do banco por operações de pagamento não autorizadas no online banking…", cit., p. 193.

individuais e sucessivas, e que pode enunciar as obrigações e condições para a abertura de uma conta de pagamento[173], ou seja, como muito bem explica Maria Raquel Guimarães, o contrato-quadro deve ser entendido com um contrato que antecipa as regras que regem a conduta de cada uma das partes nos contratos subsequentes – mandatos de pagamento – em que é utilizado o instrumento de pagamento, permitindo assim, a uniformização e consequente mecanização da celebração dos subsequentes contratos[174]. À semelhança do que se verifica no atual regime (DSP2), na PRSP o legislador prevê um conjunto de deveres de informação distintos[175] consoante estejam em causa operações de pagamento que ocorram isoladamente[176], ou operações de pagamento enquadradas no âmbito de um contrato-quadro[177], e bem assim, um núcleo de regras comuns[178], que disciplinam os direitos e os deveres das partes e especificam o regime de repartição do risco de fraude, entre eles[179]. No que concerne ao contrato-quadro, à semelhança do que verificamos na DSP2, na PRSP o legislador faz a distinção entre as informações que devem ser fornecidas ao utilizador antes da celebração do contrato-quadro, e as informações que devem ser prestadas relativas às transações durante a sua execução, fornecidas antes e depois da sua realização, atenta a necessidade de prestar clarificações ao utilizador nas diferentes fases da operação[180]. Não obstante a celebração do contrato-quadro num determinado momento, o utilizador encontra-se ainda protegido por uma série de deveres de informação a que o prestador de serviços de pagamento fica adstrito no âmbito dos contrato-

[173] Corresponde ao artigo 4.º, n.º 21 da DSP2.

[174] Maria Raquel Guimarães acrescenta ainda que o "*contrato-quadro é um contrato não negociado, elaborado unilateralmente, a que o utilizador do instrumento de pagamento adere "em bloco", sob pena de não aceder ao serviço prestado*", em "Serviços de pagamento e instrumentos de pagamento: evoluções recentes", in *Estudos de direito do consumo*, volume II, Rui Mascarenhas Ataíde, Francisco Rodrigues Rocha, Vítor Palmela Fidalgo (org.), Coimbra, Almedina, 2023, pp. 737-753; cit. p. 140. A respeito do "*desdobramento contratual*", ver também Maria Raquel Guimarães, em *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos*, Coimbra Editora, 2011; no mesmo sentido em "The debit and credit card framework contract and its influence on European legislative initiatives", in *InDret Comparado, Revista para el Análisis del Derecho*, 2012, n.º 2; e também sobre este tema, em "*La Directiva (UE) 2015/2366, sobre servicios de pago (DSP2) y los pagos electrónicos*", cit.. Em sentido contrário, Francisco Mendes Correia entende que as "*operações de pagamento individuais devem qualificar-se como atos de execução do contrato inicial e não como novos contratos*", em "Operações não autorizadas e o Regime jurídico dos serviços de pagamento e da moeda eletrónica", cit., p. 705.

[175] De acordo com o considerando 46 da PRSP, com equivalência ao considerando 57 da DSP2.

[176] Artigo 11.º a 17.º da PRSP e artigo 43.º a 49.º da DSP2

[177] Artigo 18.º a 26.º da PRSP e artigo 50.º a 58.º da DSP2

[178] Artigo 4.º a 10.º da PRSP e artigo 38.º a 42.º da DSP2.

[179] Cfr. Mafalda Miranda Barbosa, em "Serviços de pagamentos, repartição do risco e responsabilidade civil…", cit., p. 654.

[180] Maria Raquel Guimarães em "*La Directiva (UE) 2015/2366, sobre servicios de pago (DSP2) y los pagos electrónicos*", cit., pp. 8 e 9. Neste sentido, o quadro normativo prevê as informações a prestar antes da execução de operações individuais (já após estar vinculado por um contrato-quadro), *cfr.* artigo 24.º da PRPS e artigo 56.º da DSP2; as informações a prestar ao ordenante sobre as operações de pagamento individuais (depois de o montante ter sido debitado da conta do ordenante)- artigo 24.º da PRPS e artigo 56.º da DSP2; e bem assim, as informações a prestar ao beneficiário sobre operações de pagamentos individuais (após a execução de uma operação de pagamento)- artigo 25.º da PRSP e artigo 57.º da DSP2.

subsequentes. Este é um ponto fulcral para acautelar a devida proteção dos utilizadores, na medida em que, os deveres de informação que recaem sobre o prestador de serviços de pagamento, em caso algum, se esgotam no contrato "inicial".

O legislador europeu continua (e nem de outra forma se poderia equacionar) a manter o princípio do consentimento para a realização das operações de pagamento[181]. Podemos dizer que se trata de um *double check*, isto é, o legislador impõe que o utilizador seja chamado, num segundo momento, a autorizar uma operação solicitada[182]. Conforme facilmente se depreende, esta regra assume enorme importância como medida de proteção do utilizador e como mecanismo de prevenção de eventuais situações de fraude. Não obstante o momento e os meios de aprovação possam ter sido definidos em momento prévio — no âmbito do contrato-quadro —, certo é que, cada operação, carecerá, sempre, de uma (nova) autorização, não fazendo sentido que, uma autorização genérica, concedida *ab initio*, no âmbito do contrato-quadro, pudesse ter valor *ad aeternum.* A lei exige uma renovação da vontade do usuário do serviço[183]. De forma a clarificar este regime, a PRSP passa a contemplar também neste normativo os prestadores de serviços de informação sobre contas e os prestadores serviços de iniciação de pagamento, a quem só será permitido o acesso a determinadas contas se o utilizador dos serviços de pagamento tiver expressamente autorizado esse acesso, sendo que a ausência de autorização deverá considerar-se como não autorização (tema já abordado anteriormente). Entendemos que não poderia ser de fora diferente, pelo que, muito bem andou o legislador ao aqui contemplar os prestadores de serviços de informação sobre contas e os prestadores de iniciação de pagamento.

Por seu turno, o prestador de serviço que gere a conta, não pode recusar a execução de uma ordem de pagamento autorizada, a não ser que não estejam reunidas todas as condições definidas no contrato-quadro[184]. Significa isto que, cabe ao prestador de serviços de pagamento validar a conformidade da ordem de pagamentos recebida e confirmar a mesma através da sua execução. Entende-se, portanto, que neste momento, é o prestador de serviços de pagamento

[181] Artigo 49.º da PRSP e artigo 64.º da DSP2. De referir que o Parlamento propõe a inclusão no artigo 3.º da PRSP da definição de "Autorização", que deve ser entendida como a autorização por um utilizador de serviços de pagamento da execução de uma operação de pagamento ou do acesso a dados de informação sobre contas, conforme considerando 65-A da Resolução legislativa do Parlamento Europeu (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD))

[182]Maria Raquel Guimarães fala em "*dupla manifestação de vontade*" - as partes são chamadas a renovar a sua vontade de contratar sempre que se pretenda realizar uma nova operação de pagamento automático, em *O Contrato-Quadro no Âmbito da Utilização de Meios de Pagamento Electrónicos*, Coimbra Editora, 2011, p. 465.

[183] Cfr. Maria Raquel Guimarães em *"La Directiva (UE) 2015/2366, sobre servicios de pago (DSP2) y los pagos electrónicos*", cit., p. 9.

[184] Artigo 79.º, n.º 2 da PRSP e artigo 79.º, n.º 2 da DSP2

convidado a renovar a sua vontade de contratar[185]. Ora, é em função dos direitos e obrigações relativos à prestação e utilização dos serviços de pagamento que será apurada e imputada a concreta responsabilidade dos agentes pelos prejuízos no âmbito das operações de pagamento não autorizadas.

4.1. OPERAÇÕES DE PAGAMENTO NÃO AUTORIZADAS

Não obstante o crescente aumento do recurso aos pagamentos eletrónicos, a verdade é que os mesmos continuam assombrados pelo risco de fraude, tantas vezes falado e noticiado nos meios de comunicação social[186]. Conforme já referimos, a veloz evolução tecnológica beneficia também os agentes fraudulentos, na medida em que recorrem cada vez mais a mecanismos de tecnologia de ponta, mas também, de *engenharia social*, dos quais emergem novas formas de fraude, dificilmente detetáveis, assim como, esquemas cada vez mais rebuscados, de difícil acompanhamento e prevenção[187]. Atendendo aos meios empregues, a criminalidade associada à fraude, no âmbito dos serviços de pagamento, é caracterizada por um grau considerável de anonimato: uma operação de pagamento não autorizada, executada por um banco português, por conta de um utilizador de serviços de pagamento português, pode ser fraudulentamente desencadeada por um agente a milhares de quilómetros de distância, sendo os fundos transferidos para uma conta bancária numa terceira jurisdição.

Nesta medida, atenta a vulnerabilidade dos utilizadores quanto a esta matéria, a regulamentação dos pagamentos não autorizados é um tema complexo, gerador de constante preocupação legislativa, bem como de ampla análise e discussão da jurisprudência e da doutrina nacional[188], e, por conseguinte, também merecedor da nossa análise mais cuidada,

---

[185] Mais uma vez, cfr. Maria Raquel Guimarães em "*La Directiva (ue) 2015/2366, sobre servicios de pago (DSP2) y los pagos electrónicos*", cit. p. 9.

[186] Cerca de 27% dos indivíduos inquiridos nunca efetuaram compras pela Internet, sendo que muitos deles justificam este facto com a «preocupações com a segurança e privacidade dos pagamentos» na realização das compras ou encomendas online (45% em Portugal face a 14% na média da UE), em *O comércio eletrónico em Portugal e na União Europeia- Segmento residencial e empresarial- Relatório de 2021*, ANACOM- Autoridade nacional de comunicações, pp. 8-18, disponível em <ComercioEletronico2021_final.pdf (anacom.pt)>(26-05-2024).

[187] Maria Raquel Guimarães, "Pagamentos electrónicos não autorizados e fraudulentos", cit., p. 227.

[188] Referimos alguns exemplos, entre muitos: Maria Raquel Guimarães, "«Na minha Conta ou na tua?»…", cit., pp.57-120; Maria Raquel Guimarães e Reinhard Steennot, "Allocation of liability in case of payment fraud: who bears the risk of innovation? A comparison of Belgian and Portuguese law in the context of PSD2", *in European Review of Private Law*, Volume 30, Issue 1, 2022, pp. 29-72; Francisco Mendes Correia,, "Responsabilidade e Risco nas operações de pagamentos não autorizadas", *in Revista da Faculdade de Direito da Universidade de Lisboa*, (2023), pp. 417-466; Mafalda Miranda Barbosa, em "Serviços de pagamentos, repartição do risco e responsabilidade civil…", cit. pp. 622 a 682; Miguel Pestana Vasconcelos, "A responsabilidade do banco por operações de pagamento não autorizadas no online banking…", cit., pp. 191-208.

desta feita, à luz da nova proposta de regulamento dos serviços de pagamento, que não parece apresentar alterações de fundo face ao anterior regime, conforme veremos adiante[189].

No que concerne à distribuição dos prejuízos por operações de pagamento não autorizadas, esta continuará a assentar no princípio da repartição do risco, baseado nas condutas das partes bancárias[190], isto é, na violação dos deveres que as vinculam[191]. Nas palavras de Francisco Mendes Correia[192], o risco relevante não é o do perecimento de certas coisas monetárias, mas antes o risco de interferência de terceiro ou de falha técnica nos sistemas dos bancos, que poderia, eventualmente, ter sido evitado pela conduta de um ou algum dos contraentes[193]. Assim, o legislador parece aceitar que, estando em causa um risco potencial e previsível, passível de ser contornado através de rígidas medidas de proteção, que deverão ser garantidas pelos prestadores de serviços de pagamentos, o critério para apuramento da responsabilidade deverá assentar numa ponderação dos deveres violados[194]. A repartição do risco objetivamente considerado só operará quando não possa ser imputada a responsabilidade ao prestador de serviços de pagamento ou ao utilizador, com base em critérios subjetivos, isto é, é exigida uma prévia análise subjetiva de eventuais deveres preteridos pelos contraentes.[195]

De igual modo, no que concerne ao regime de responsabilidade e distribuição do risco, o legislador europeu continua a consagrar um regime que não dispensa o recurso a normas e conceitos de direito nacional, em matéria de cumprimento de obrigações e responsabilidade

[189] Artigo 71.º da DPS2 e artigo 54.º da PRSP.
[190] Cfr. explica Mafalda Miranda Barbosa, em "Serviços de pagamentos, repartição do risco e responsabilidade civil…", cit., p. 648.
[191] Referente a esta temática, *vide* também, Francisco Mendes Correia, "*Operações não autorizadas e o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica*", cit., pp. 719 a 721. Nas palavras de Patrícia Guerra, trata-se de um "*um regime especial de responsabilidade civil pelo risco*", em "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", *Revista Electrónica de Direito*, N.º 2, junho 2016, p. 51. A este respeito, referir que, a responsabilização de terceiros, não é, na maioria das vezes, uma alternativa viável, sendo, inclusive, de difícil fundamentação jurídica, conforme defende Mafalda Miranda Barbosa, em "Serviços de pagamentos, repartição do risco e responsabilidade civil…", cit., pp. 628 a 639.
[192] Francisco Mendes Correia, "Responsabilidade e Risco nas operações de pagamentos não autorizadas", *in Revista da Faculdade de Direito da Universidade de Lisboa*, cit., p. 438.
[193] Também neste sentido, Mafalda Miranda Barbosa, em "Serviços de pagamentos, repartição do risco e responsabilidade civil…", cit., p. 648.
[194] Idem, e também Francisco Mendes Correia, "Responsabilidade e Risco nas operações de pagamentos não autorizadas", cit., p. 438.
[195] Diferente do regime geral, em que opera uma repartição objetiva do risco, devendo ser onerado quem se encontra mais "exposto" ao risco de perecimento da coisa – *cfr*. artigo796.º do C.C.

civil[196], nomeadamente, no que respeita à avaliação e integração de conceitos como *atuação fraudulenta, dolo ou negligência grosseira*[197].

Não obstante o princípio da repartição do risco consagrado no regime que tutela as operações de pagamento não autorizadas, o cliente consumidor continua a ser merecedor de especial tutela por parte do legislador, na medida em que continua a ser encarado como o "elo mais fraco" da relação contratual[198]. O legislador considera que, embora o prestador de serviços de pagamento possa também ser vítima de fraude[199], este dispõe de mais recursos para o combate e prevenção da mesma. Esta especial tutela encontra-se bem patente em todo o regime da responsabilidade por operações não autorizadas, nomeadamente, no que concerne ao ónus da prova[200], ao critério de imputação objetiva da responsabilidade por perdas[201], e bem assim, na obrigação que recai sobre o prestador de serviços de pagamento pelo reembolso imediato ao ordenante do montante da operação de crédito não autorizada, conforme veremos com maior pormenor adiante.

4.1.1. **Responsabilidade do prestador de serviços de pagamento**

O princípio base em matéria de responsabilidade da PRSP é muito semelhante ao previsto na DSP2: perante uma operação de pagamento não autorizada, o prestador de serviços de pagamento deve reembolsar, imediatamente, o ordenante, pelo montante dessa operação, até ao final do primeiro dia útil seguinte a ter tido conhecimento da operação não autorizada, ou, após esta lhe ter sido comunicada[202]. Este reembolso não estará "dependente da comunicação

---

[196] À semelhança do que verificamos no regime consagrado na DSP2. A este respeito, *vide*, Francisco Mendes Correia, "Responsabilidade e Risco nas operações de pagamentos não autorizadas", cit., p. 438.

[197] O considerando 82 da PRSP concretiza que para avaliar a eventual negligência ou negligência grave deverão ser tidas em conta todas as circunstâncias, devendo os elementos de prova e o grau da alegada negligência ser avaliados nos termos do direito nacional.

[198] Neste sentido o considerando 75 da PRSP.

[199] Nomeadamente, em caso de usurpação de identidade.

[200] Artigo 55.º da PRSP- caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada ou alegue que a referida operação não foi corretamente executada, cabe ao prestador de serviços de pagamento fazer prova de que a operação de pagamento foi autorizada, devidamente registada e contabilizada, e de que não foi afetada por qualquer avaria técnica ou por outra deficiência do serviço prestado pelo prestador de serviços de pagamento.

[201] A este respeito, Vide Acórdão do Tribunal da Relação de Coimbra, de 10-12-2020, Relator Emídio Santos, segundo o qual "*Não havendo prova da culpa, nem do utilizador, nem do prestador do serviço, o regime jurídico dos serviços de pagamento constante do anexo I ao Decreto-Lei ao Decreto-Lei n.º 317/2009, de 30 de Outubro, com as alterações que lhe foram introduzidas pelo Decreto-Lei n.º 242/2012, de 7 de Novembro, e pelo Decreto-Lei n.º 157/2014, de 24 de Outubro, fazia recair a responsabilidade pelo reembolso do montante da operação sobre o prestador do serviço.*";

[202] Artigo 56.º, n.º 1 da PRSP e artigo 73.º, n.º 1 da DSP2. De acordo com o artigo 56.º, n.º 3 "*o prestador de serviços de pagamento do ordenante deve repor a conta de pagamento debitada na situação em que estaria se a operação de pagamento não autorizada não tivesse sido executada*", e continua, (n.º 6) "*O ordenante pode ter direito a uma indemnização financeira adicional por parte do prestador de serviços de pagamento, nos termos do direito aplicável ao contrato celebrado entre o ordenante e o prestador de serviços de pagamento, ou do*

atempada" (ou da justificação do atraso) da ocorrência de uma operação não autorizada, e é exigível mesmo nos casos em que a comunicação não seja realizada diligentemente, contrariamente ao que tem vindo a ser entendido pelos prestadores de serviços de pagamento[203]. Mantém-se a regra de que as operações não autorizadas (ou incorretamente executadas) devem ser comunicadas dentro de um prazo nunca superior a 13 meses[204].

A primeira exceção ocorre, desde logo, no caso em que o prestador de serviços de pagamento tem motivos razoáveis para suspeitar de fraude cometida pelo ordenante[205]. Ora, perante esta circunstância, e à luz da PRSP, cabe ao prestador de serviços de pagamento, no prazo de 10 dias úteis, a contar da data que tomou conhecimento da operação não autorizada em causa[206], e após uma investigação complementar, proceder ao efetivo reembolso ao ordenante, ou, em alternativa, apresentar uma justificação de recusa de reembolso e indicar ao utilizador os organismos para quem poderá remeter a sua reclamação[207] em caso de discórdia com a posição do prestador do serviço de pagamento[208]. O prestador de serviços de pagamento terá a oportunidade de realizar uma investigação prévia; não obstante, terá de apresentar os

contrato celebrado entre o ordenante e o prestador do serviço de iniciação do pagamento, conforme aplicável", ou seja, que o dano direto deve ser ressarcido através da reposição/reconstituição natural da conta, sendo mecanismos "*claramente indemnizatórios, manifestando o princípio da reconstituição natural, presente no artigo 562..º do Código Civil*", *cfr.* defende Francisco Mendes Correia, em "Operações não autorizadas e o Regime jurídico dos serviços de pagamento e da moeda eletrónica", cit., p. 711.

[203] Cit. Maria Raquel Guimarães, "«Na minha Conta ou na tua?»…", cit., p.72.

[204] Cit. Maria Raquel Guimarães, "«Na minha Conta ou na tua?»…", cit., p. 68, e em conformidade com EBA/Op/2022/06, 290-291. Ainda sobre esta temática, cumpre fazer referência à decisão do Tribunal de Justiça, (Ac.TJ, 2-set.-2021, Processo C-337/20, DM, LR c. Caise régionale de Crédit agricole mutuel (CRCAM)- Alpes-Provence, n.°34), no sentido que, ainda ao abrigo da Diretiva 2007/64, no que concerne ao prazo de treze meses para comunicação da operação não autorizada em causa, a responsabilidade do prestador desses serviços só pode ser aferida à luz da Diretiva em causa, e portanto, o prazo estipulado tem carácter imperativo, não podendo o utilizador efetivar a responsabilidade do prestador de serviços de pagamento com base num regime de responsabilidade diferente do previsto ao abrigo da Diretiva em questão.

[205] A este respeito, o legislador não deixou margem para dúvidas quando refere expressamente "*fraude cometida pelo ordenante*". Ora, esta questão foi alvo de reflexão doutrinal, na medida em que o artigo 73.º da DSP2 apenas refere que prestador do serviço poderá não reembolsar "*se o prestador de serviços de pagamento do ordenante tiver motivos razoáveis para suspeitar de fraude*", não concretizando se fraude de terceiro ou do cliente. No entanto, nem outra interpretação faria sentido, uma vez que, de outro modo, o dever de reembolso por pagamentos não autorizados nunca existiria, tendo em consideração que, na maioria das vezes, está em causa um comportamento fraudulento de um terceiro, *cfr*. refere Maria Raquel Guimarães em "«Na minha Conta ou na tua?»…", cit., p. 71; e no mesmo sentido, também, Maria Raquel Guimarães e Reinhard Steennot, em "Allocation of liability in case of payment fraud: who bears the risk of innovation?...", cit., pp. 41 a 44. Acompanha este entendimento Patrícia Guerra, em "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", cit., p.28.

[206] O Parlamento Europeu propõe a alteração deste prazo para 14 dias, *cfr.* Resolução legislativa do Parlamento Europeu (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)), não obstante, aguarda-se ainda a posição do Conselho em primeira leitura.

[207] Nos termos dos artigos 90.º, 91.º, 92.º, 93.º, 94.º e 95.º da PRSP. Também nesta matéria o Parlamento sugere uma alteração à letra da lei, com vista a concretizar os termos da justificação de recusa a apresentar pelo PSP, devendo a mesma ser exata e fundamentada, e apresentada por escrito à autoridade competente, *cfr.* resolução legislativa do Parlamento Europeu (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD))

[208] Artigo 56.º, n.º 2 da PRSP.

motivos e os elementos comprovativos que justifiquem a recusa de reembolso, não sendo suficiente a simples convicção ou suspeita de um comportamento fraudulento[209].

Continua sem estar previsto um critério de diligência especial para os bancos, para além dos deveres e obrigações previstas no quadro regulamentar. Assim, sempre se dirá que a responsabilidade do prestador de serviços de pagamento só poderá ser afastada perante a apresentação de elementos que demonstrem a efetiva existência de fraude ou negligência grave por parte do utilizador de serviços de pagamento. Ora, o ónus da prova continua a recair sobre o prestador de serviços de pagamento[210].

Conforme já referimos, esta opção legislativa espelha uma especial tutela que o legislador pretende conferir ao utilizador/consumidor, na medida em que o banco assume aqui a posição dominante[211]. Isto é, o banco dedica-se a título profissional à atividade de prestação de serviços de pagamentos, pelo que deverá recair sobre si o ónus de evitar o risco das operações não autorizadas[212], sendo expectável que, com uma maior responsabilização dos bancos, estes assumam critérios e mecanismos mais eficientes e rigorosos contra a fraude. Assim, mesmo quando não haja qualquer culpa por parte do prestador do serviço, o risco há de correr por conta dele[213].

É de referir que, ainda que a operação de pagamento seja iniciada através de um prestador de serviços de iniciação de pagamentos, o reembolso ao utilizador sempre caberá ao prestador de serviços de pagamento que gera contas[214], não obstante o posterior direito de regresso sobre o primeiro, cabendo a este o ónus da prova de que a operação de pagamento foi autorizada e devidamente registada, e não foi afetada por nenhuma avaria técnica ou por uma deficiência relacionada com o serviço de pagamento pelo qual é responsável[215].

Não sendo afastada a responsabilidade do prestador de serviços de pagamento pela operação de pagamentos não autorizada, o utilizador poderá ainda exigir uma indemnização

---

[209] *Cfr*. considerando 77 da PRSP.
[210] Artigo 55.º da PRSP e artigo 72.º da DSP2.
[211] Francisco Mendes Correia, justifica em "Operações não autorizadas e o Regime jurídico dos serviços de pagamento e da moeda eletrónica", *Revista de Direito Civil*, cit., pp. 719 e 720.
[212] Idem, p. 455.
[213] Mafalda Miranda Barbosa, em "Serviços de pagamentos, repartição do risco e responsabilidade civil…", in *Revista de Direito Comercia*l, cit., pp. 666 e 667.
[214] Artigo 56.º, n.º 4 e 5 da PRSP e artigo 73.º, n.º 2 da DSP2.
[215] A este respeito, Francisco Mendes Correia refere que "*a intervenção de um prestador de serviços de iniciação não afeta os dois principais direitos do ordenante, em caso de operações não autorizadas: o reembolso imediato do montante da operação e a reposição da conta no estado em que estaria, na sua ausência*", e sublinha a intenção do legislador em favorecer os serviços de iniciação de pagamento, na medida em que, numa fase inicial, os "desonera" de responsabilidade, uma vez que, "*o ordenante já está suficientemente protegido com a intangibilidade da sua pretensão, a exercer contra o prestador que gere a conta, mesmo em caso de intervenção de um iniciador*", *in* "Os novos serviços de iniciação de pagamentos: algumas notas sobre a responsabilidade civil" - *in Estudos de direito do consumo*, volume II, pp. 761 e 762.

financeira adicional, por força contratual, nos termos do artigo56.º, n.º 6, da PRSP. Vão neste sentido algumas decisões dos tribunais portugueses, no âmbito das quais, mesmo perante a imputação objetiva da responsabilidade ao banco (isto é, sem conduta merecedora de censura), os tribunais procederam à fixação de indemnizações por danos consequenciais[216].

Carece ainda de sublinhar que, conforme vimos, a imputação da responsabilidade ao PSP poderá ocorrer com base num critério meramente objetivo, isto é, não estando em causa nenhum comportamento que acarrete responsabilidade do utilizador, o sistema da imputação prescindirá de um juízo de ilicitude, e a imputação de perdas far-se-á a título objetivo, recaindo sobre o banco[217]. Poderão, por exemplo, ocorrer casos em que o banco procede à correta autenticação e registo da operação, não existindo elementos para tecer um juízo de censura sobre o prestador, sendo, ainda assim, as perdas imputadas, objetivamente, ao banco. Não obstante, posteriormente, o banco poderá tentar recuperar esses prejuízos junto do terceiro infrator. Estamos nestes casos perante "um conjunto de normas que pode ser reconduzido ao modelo de responsabilidade pelo risco ou responsabilidade objetiva"[218].

a. **(Isenção) da autenticação forte do utilizador**

A dimensão do artigo 85.º da PRSP espelha bem a preocupação do legislador em abarcar maior clareza a esta matéria da autenticação forte, procurando elencar as operações de pagamento incluídas e excluídas dos requisitos de autenticação forte, em clara consonância com a recomendação da EBA[219].

A regra da distribuição dos prejuízos no âmbito das operações de pagamento não autorizadas continua a ser derrogada nos casos em que o prestador de serviços de pagamento não exigir a autenticação forte do ordenante, à semelhança do previsto na DSP2[220]. Importa, no entanto, fazer referência ao conjunto de operações de pagamento em relação às quais o legislador, taxativamente, isentou da aplicação da autenticação forte. Neste sentido, o

[216] A este título, veja-se por exemplo a decisão do Tribunal da Relação de Lisboa, de 15 de março de 2016 (Rijo Ferreira) que imputou ao Banco a responsabilidade por dano reputacional, tendo fixado uma indemnização a pagar ao cliente no valor de € 7.500,00; No mesmo sentido, o Acórdão da Relação do Porto, de 13 de Junho de 2018 (Francisca Mota Vieira). Francisco Mendes Correia considera excessiva esta tutela concedida pelos tribunais, na medida em que transcendem o núcleo dos riscos coberto pela imputação objetiva, *in* "Operações não autorizadas e o Regime jurídico dos serviços de pagamento e da moeda eletrónica", cit., p. 725, onde defende que incumbe aos Tribunais identificar o modelo de imputação das perdas ao Banco, que nem sempre resultam claros.

[217] Acórdão da Relação do Porto, de 13 de junho de 2018 (Francisca Mota Vieira).

[218] *Cfr.* Francisco Mendes Correia, em "Operações não autorizadas e o Regime jurídico dos serviços de pagamento e da moeda eletrónica", cit., p. 719.

[219] Veja-se que o artigo 85.º da PRSP abarca 12 pontos, ao passo que o artigo 97.º na DSP2, sobre a mesma matéria, contempla apenas 5 pontos. A EBA propôs que a diretiva introduzisse requisitos específicos em relação às exclusões da aplicação do SCA especificadas no considerando 95, tais como as operações de pagamento em papel, os MOTOs e em relação à utilização de MIT - EBA/Op/2022/06, n.º 322, p. 75.

[220] Artigo 60.º, n.º 2 da PRSP e artigo 74.º, n.º 2, da DSP2.

legislador começa desde logo por fazer referência às operações de pagamento que sejam iniciadas "apenas pelo beneficiário", que não estão sujeitas a uma autenticação forte do cliente — caso dos débitos diretos[221] — desde que sejam iniciadas sem interação ou intervenção do ordenante[222]. Esta isenção será afastada sempre que o mandato conferido ao beneficiário for concedido através de um canal remoto, com a intervenção direta de um prestador de serviços de pagamento na instituição desse mandato, caso em que já deve ser aplicada a autenticação forte, nos termos do artigo 85.º, n.º 6, PRSP. A este respeito, há que ressalvar que, em relação às operações de pagamento em que o montante não seja antecipadamente conhecido e os fundos estejam bloqueados num instrumento de pagamento, o legislador veio introduzir a obrigação legal de "o beneficiário informar o PSP do montante exato da operação de pagamento imediatamente após a entrega do serviço ou dos bens ao ordenante", bem como, estabelecer um principio de proporcionalidade entre o montante dos fundos bloqueados e o montante da futura operação de pagamento que possa "razoavelmente prever-se no momento do bloqueio dos fundos"[223]. Ora, no âmbito destas operações, os critérios para reembolso ao ordenante resultam nos exatos termos do previsto na DSP2, isto é, o ordenante poderá solicitar o reembolso ao prestador de serviço de pagamento, através de pedido apresentado dentro do prazo de oito semanas a contar da data em que os fundos foram debitados, nos casos em que o montante exato da operação de pagamento não foi especificado no momento em que a autorização concedida, e o montante transferido para o beneficiário exceda o montante que o ordenante poderia "razoavelmente esperar", atendendo ao seu histórico de despesas, aos termos do contrato-quadro, bem como, às circunstâncias específicas do caso[224].

Bem assim, o legislador vem esclarecer que não estão sujeitas a autenticação forte do cliente as operações de pagamento no âmbito das quais o ordenante "emite ordens de pagamento em modalidades diferentes da utilização de plataformas ou dispositivos eletrónicos, tais como ordens de pagamento em suporte papel, ordens postais ou ordens telefónica", ainda que as mesmas sejam realizadas por via eletrónica[225]. No entanto, caberá ao prestador de serviços de pagamento garantir os requisitos e os controlos de segurança que permitam uma

[221] Nos termos do artigo 3.º, n.º 27, débito direto é definido como "*um serviço de pagamento que consiste em debitar a conta de pagamento de um ordenante, sendo a operação de pagamento iniciada pelo beneficiário com base num mandato conferido pelo ordenante ao beneficiário, ao prestador de serviços de pagamento do beneficiário ou ao prestador de serviços de pagamento do próprio ordenante*".
[222] Artigo 85.º, n.º 2, da PRSP.
[223] Artigo 61.º da PRSP e artigo 75.º da DSP2 e texto introdutório da PRSP, p. 11.
[224] Artigo 62.º da PRSP e artigo 76.º da DSP2. A este respeito, *Vide* Francisco Rodrigues Rocha, "Débitos directos. aspectos de regime de protecção do consumidor" - in *Estudos de direito do consumo*, volume II, Rui Mascarenhas Ataíde, Francisco Rodrigues Rocha, Vítor Palmela Fidalgo (org.), Coimbra, Almedina, 2023, pp. 773-885
[225] Artigo 85.º, n.º 7 da PRSP.

forma de autenticação da operação de pagamento[226]. Esta temática não se encontrava cabalmente esclarecida no âmbito da DSP2, gerando dúvidas quanto à exigência da autenticação forte, às quais a PRSP pretende agora dar resposta[227].

Nos termos do Regulamento Delegado (EU) 2018/389, os prestadores de serviços de pagamento podem aplicar isenção de requisitos de autenticação forte quando estejam em causa operações de pagamento sem contacto (*tecnologia contactless ou NFC*) até ao montante de 50 euros, com um máximo acumulado de 150 euros, ou de 5 operações[228]. Com vista a colocar cobro a interpretações divergentes[229], o legislador refere expressamente na PRSP[230] que, caso o prestador de serviço de pagamento aplique uma isenção da aplicação da autenticação forte do cliente, o ordenante só responderá por eventuais perdas se tiver atuado de forma fraudulenta[231], recaindo o ónus de prova sobre o prestador de serviços de pagamento.

Ainda em relação à autenticação forte, tendo em consideração o resultado da avaliação da DSP2, que apontou para a existência de problemas de aplicação deste mecanismo, o que, inclusive, motivou o adiamento da sua aplicação de 2018 para 2020[232], o legislador veio agora propor novas disposições relativas à responsabilidade dos prestadores de serviços técnicos e dos operadores de sistemas de pagamento, passando a responsabilizá-los por quaisquer prejuízos causados aos beneficiários, aos prestadores de serviço de pagamento do beneficiário, ou ao prestador de serviço de pagamento do ordenante, pela não prestação dos serviços necessários para garantir a aplicação da autenticação da forte[233].

---

[226] Neste sentido o considerando 108 da PRSP.

[227] EBA/Op/2022/06, n.º 320, p. 75: "*A exclusão da aplicação do SCA para operações de pagamento não eletrónicas revelou-se difícil de aplicar e supervisionar na prática com base na atual formulação do presente considerando (...)".* Também Maria Raquel Guimarães em "«Na minha Conta ou na tua?»…", cit., p. 98 e 99.

[228] Artigo 11.º do Regulamento Delegado (EU) 2018/389.

[229] Maria Raquel Guimarães e Reinhard Steennot, defendiam já que a possibilidade realização de pagamentos de baixo valor através de tecnologia de leitura por aproximação (NFC — *near field communication*) constitui uma funcionalidade incorporada num instrumento de pagamento ou numa aplicação de pagamento, que o titular pode escolher utilizar ou não em cada operação, e não um novo instrumento de pagamento distinto do instrumento de pagamento em que está incorporada, nomeadamente um "instrumento de pagamento de baixo valor", *in* "Allocation of liability in case of payment fraud: who bears the risk of innovation?...", cit., p. 40. Distinto foi o entendimento do TJUE, Processo C-287/19, DenizBank AG, 11 de Novembro de 2020, ECLI:EU:C:2020:897, § 75, onde se diz que a utilização da função NFC de um cartão bancário representa um conjunto de procedimentos não personalizados que deve ter sido acordado entre o utilizador e o prestador de serviços de pagamento e que são utilizados para iniciar uma ordem de pagamento, pelo que esta função constitui um 'instrumento de pagamento', na aceção do artigo 4.º, ponto 14, segunda hipótese, da Diretiva 2015/2366", referido por Maria Raquel Guimarães, em "«Na minha Conta ou na tua?»…", cit., p. 94.

[230] Também neste sentido, no considerando 22 da PRSP: "*A NFC deve, por conseguinte, ser entendida como uma funcionalidade de um instrumento de pagamento e não como um instrumento de pagamento enquanto tal*".

[231] Artigo 60.º, n.º 2 da PRSP.

[232] Conforme referido na parte introdutória da PRSP, p. 11.

[233] Artigo 58.º da PRSP. Na proposta de alteração do Parlamento Europeu, é sugerida a inclusão na letra da Lei de um limite desta responsabilidade ao montante da operação em questão- Resolução legislativa do Parlamento Europeu (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)).

4.1.2. Responsabilidade do ordenante

No que respeita à imputação da responsabilidade ao utilizador dos serviços de pagamento, por operações bancárias não autorizadas, o legislador continua a consagrar o modelo dual[234], isto é, o utilizador será responsabilizado em duas situações: em relação às perdas relativas a operações de pagamento não autorizadas resultantes da utilização de um instrumento de pagamento perdido ou furtado ou alvo de apropriação abusiva, o utilizador será responsável até ao montante máximo de €50,00[235], e bem assim, será responsável por suportar todas as perdas relativas a operações de pagamento não autorizadas sempre que tenha atuado de forma fraudulenta ou com incumprimento, com dolo ou por negligência grave, de uma ou mais obrigações a que esteja adstrito[236]. Não obstante, ambos os casos comportam exceções, que não foram esquecidas no âmbito PRSP.

a. Operações de pagamento não autorizadas resultantes da utilização de um instrumento de pagamento perdido ou furtado ou alvo de apropriação abusiva

Ao compararmos os dois preceitos legais — o artigo 60.º da PRSP e o artigo 74.º da DSP2, verificamos desde logo total identidade na responsabilização do utilizador do serviço de pagamento, até ao montante máximo de € 50,00, por perdas relativas a operações de pagamento não autorizadas resultantes da utilização de um instrumento de pagamento perdido ou furtado ou alvo de apropriação abusiva. Nesta medida, o utilizador de serviços de pagamento continuará a estar obrigado a comunicar ao prestador de serviços de pagamento, "sem demora indevida e logo que tenha tomado conhecimento dos factos"[237] a perda, o furto, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento. Cumprida a comunicação ao prestador de serviços de pagamento, e após essa data, o ordenante não mais será responsabilizado por posteriores consequências financeiras resultantes da utilização de um instrumento de pagamento perdido, roubado ou abusivamente apropriado, conforme já previsto na DSP2[238]. Do mesmo modo, fica afastada a responsabilidade do utilizador, quando o PSP não

---

[234] *Cfr.* refere Francisco Mendes Correia, "Responsabilidade e Risco nas operações de pagamentos não autorizadas", cit., p. 441.

[235] Mantem-se inalterado o valor consagrado na DSP2, a fim de incentivar o utilizador do serviço de pagamento a notificar o prestador do serviço de pagamento de qualquer furto ou perda de um instrumento de pagamento*, cfr.* considerando77 da PRSP.

[236] Artigo 60.º da PRSP e artigo 74.º da DSP2. Francisco Mendes Correia, aponta três níveis de censura distintos, um primeiro nível não qualificado; um segundo nível em caso de negligência grave; e um terceiro nível em que o incumprimento é deliberado ou existe atuação fraudulenta do utilizador. *Cfr.* " em "Operações não autorizadas e o Regime jurídico dos serviços de pagamento e da moeda eletrónica", cit., p. 715.

[237] Artigo 69.º, n.º 1 b) da DSP2 e artigo 52.º b) da PRSP.

[238] Artigo 74.º, n.º 3 da DSP2 e artigo 60.º, n.º 4 da PRSP. O ónus passa assim a recair sobre o PSP, a quem cabe a garantia de impedir a contínua utilização do instrumento de pagamento em questão. Conforme, Maria Raquel

disponibilize os meios adequados para que aquele possa comunicar as vicissitudes relativas ao instrumento de pagamento[239], conforme exigido pelo artigo 53.º, n.º 1, alínea c), salvo o caso de o utilizador ter atuado de forma fraudulenta.

Ainda à semelhança do previsto na DSP2, o legislador continua a isentar o utilizador de responsabilidade em relação a operações de pagamento não autorizadas resultantes da utilização de um instrumento de pagamento perdido ou furtado ou alvo de apropriação abusiva, quando não lhe tenha sido possível detetar a perda, o furto ou a apropriação abusiva do instrumento de pagamento antes da realização do pagamento[240], bem como, sempre que a perda do instrumento de pagamento tenha sido causada por atos ou omissões de um trabalhador, de um agente ou de uma sucursal do prestador de serviços de pagamento, ou de uma entidade à qual as suas atividades tenham sido externalizadas[241]. De sublinhar que a desresponsabilização do PSU só opera nos casos em que a fraude não era detetável, à luz do juízo do homem médio, isto é, no caso em que não era expetável que utilizador normal e devidamente prudente pudesse detetar a fraude face às circunstâncias em causa[242]. Não sendo a fraude detetável, não faria sentido imputar a responsabilidade ao utilizador, uma vez que não terá este agido com negligência grave[243]. Diferente seria, nos casos em que a fraude não foi detetada, antes da operação não autorizada, por falta de prudência e diligência do utilizador[244]. Nestes casos, justifica-se que, tendo o utilizador atuado com neglicência grave, seja responsabilizado pelas perdas ocorridas.

Guimarães, "Pagamentos eletrónicos não autorizados e fraudulentos", in *Cibercriminalidade: novos desafios, ofensas e soluções*, 2021, pp. 234 e 235; também em "A responsabilidade por operações fraudulentas no comércio electrónico", in *Direito e Informação que responsabilidade(s)?*, Ricardo Perlingeiro/Fernanda Ribeiro/Luísa Neto (orgs.), Rio de Janeiro, Editora da UFF, 2013, pp. 259-274, disponível em <Direito e Informação: que responsabilidade(s)? (Law and Information: Reciprocal Liabilities) by Ricardo Perlingeiro, Fernanda Ribeiro, Luísa Neto :: SSRN> (26-05-2024), p. 267.

[239] Artigo 60.º, n.º 4 *in fine*.

[240] Artigo 60º, n.º 1 da PRSP e artigo 74.º, n.º 1 da DSP2. Como são os casos em que o utilizador apenas se apercebe do extravio do instrumento de pagamento quando deteta a execução de operações de pagamento não autorizadas; Ver Maria Raquel Guimarães, "«Na minha Conta ou na tua?»…", cit., p. 69. Remetemos para o mesmo acórdão citado: Supremo Tribunal de Justiça, de 31 de janeiro de 2019 (Helder Almeida), que considerou intempestiva a comunicação do desaparecimento de um cartão de débito, três dias após a perda da carteira, reputando o Tribunal como negligência grave ou grosseira a violação dos deveres de diligência que recaíam sobre a Ré (utilizadora).

[241] Idem.

[242] *Cfr*. Maria Raquel Guimarães e Reinhard Steennot, em "Allocation of liability in case of payment fraud: who bears the risk of innovation?...", cit., p. 34. Também, Maria Raquel Guimarães, em "«Na minha Conta ou na tua?»…", cit., p. 75;

[243] Aliás, é isto que resulta do considerando 77 da PRSP, à semelhança do considerando 71 da DSP2. A respeito da culpa leve, Menezes Leitão, faz referência à "*conduta do agente que não seria suscetível de ser praticada por um homem médio*" *Direito das Obrigações*, I, 14.ª ed., 2017, Coimbra, Almedina, 311-313, p. 1;

[244] Ver Maria Raquel Guimarães, em "«Na minha Conta ou na tua?»…", cit., p. 75.

b. Operações de pagamento não autorizadas- fraude, dolo ou negligência grave do utilizador

A imputação subjetiva ao utilizador do serviço de pagamento ocorre quando este tenha atuado de forma fraudulenta[245], ou tenha incumprido com dolo ou negligência grave uma ou mais obrigações a que estava adstrito relativamente ao instrumento de pagamento utilizado e às credencias de segurança personalizadas[246]. Nestes casos, o utilizador suportará a totalidade das perdas ocorridas. Não obstante, à semelhança da DSP2, o legislador continua a consagrar a possibilidade de as autoridades nacionais competentes, ou os prestadores de serviços de pagamento, poderem reduzir a responsabilidade do utilizador quando este tenha atuado com "mera" negligência grave[247].

Assim, no âmbito da responsabilidade do utilizador por operações de pagamento não autorizadas, não obstante o quadro regulamentar estabelecido, o legislador europeu continua sem concretizar o que deve ser entendido por "negligência grave" ou "atuação fraudulenta"[248]. Neste sentido, cumpre lançar mão da doutrina nacional e, assim, afigura-se como "atuação fraudulenta" a intenção especial de iludir o banco para obter à sua custa uma vantagem que o utilizador sabe ser indevida[249]. Ora, por seu turno, no que respeita à atuação dolosa, convocando Menezes Cordeiro, sempre se dirá que atua com dolo aquele que de forma voluntária violar um dever em apreço, provocando um resultado lesivo[250], ou seja, o cliente é

[245] De sublinhar que, em caso de atuação fraudulenta, as imputações da totalidade das perdas ao utilizador matem-se mesmo que o banco tenha incumprido deveres em matéria de autenticação, bloqueio ou meios de comunicação, *cfr*. Francisco Mendes Correia, "Responsabilidade e Risco nas operações de pagamentos não autorizadas", *in Revista da Faculdade de Direito da Universidade de Lisboa*, cit., p. 442.

[246] Artigo 60.º, n.º 1 da PRSP e artigo 74.º, n.º 1 da DSP2.

[247] Esta possibilidade já havia sido acautelada pelo legislador nacional no âmbito do RJSPME, que prevê no artigo 115.º, n.º 4 o seguinte: "*Havendo negligência grosseira do ordenante, este suporta as perdas resultantes de operações de pagamento não autorizadas até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, ainda que superiores a (euro) 50*.". Em relação a esta temática, veja-se o Acórdão da Relação do Porto, de 08-03-2019 (Alexandra Pelayo), que, apesar de considerar a ilicitude do comportamento do banco, uma vez que não conferiu devidamente as assinaturas apostas nos contratos celebrados com a cliente, permitindo a utilização contínua do sistema de movimentação de conta da cliente (através de *homebanking*) por parte de um funcionário que não detinha poderes para o efeito, apela à presunção de culpa estabelecida pelo artigo 799.º do código civil, que determina que: "*incumbe ao devedor provar que a falta de cumprimento, ou o cumprimento defeituoso da prestação não procede de culpa sua.*", não deixando de considerar a culpa da cliente para o agravamento do resultado, em função do critério de vigilância - "*mostra-se incompatível com os deveres de diligência de um gestor criterioso a que os responsáveis da Autora se encontravam obrigados*", reduzindo a indemnização devida pelo banco (réu) em 50%.

[248] Não obstante a recomendação da EBA quanto à necessidade de serem clarificados os conceitos utilizados pela DSP2, como "*actuação fraudulenta*" e "*negligência grave*" - Autoridade Bancária Europeia (EBA), *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, cit., pp. 67-69.

[249] Cfr. Francisco Mendes Correia, "Responsabilidade e Risco nas operações de pagamentos não autorizadas", cit., p. 442.

[250] Menezes Cordeiro, *Tratado de Direito Civil, VIII*, 2ª Edição Revista e Atualizada Coimbra, Almedina, 2023.

conhecedor e está consciente das circunstâncias que integram violação do dever a que está adstrito, mas ainda assim, tem vontade de intencionalmente não o observar.

Já no que respeita ao conceito de negligência grave, o considerando 82 da PRSP disponibiliza algumas diretrizes para a integração deste conceito, segundo o qual, para além da violação de um dever de diligência, "a «negligência grave» deve significar mais do que uma mera negligência, implicando um comportamento que patenteia um grau significativo de descuido" [251], isto é, corresponde à culpa grave, entendida como a falta saliente e indesculpável, na omissão dos deveres de cuidado que só uma pessoa especialmente negligente, descuidada e incauta deixaria de observar[252]. Nas palavras de Inocêncio Galvão Teles, a culpa grave consubstancia "uma negligência grosseira" que "só por uma pessoa particularmente negligente se mostra suscetível de ser cometida"[253].

O legislador europeu mantém um patamar elevado no que respeita à relevância da negligência para responsabilização do utilizador. Assim, no que respeita à imputação ao utilizador da responsabilidade pelas perdas, no âmbito de operações não autorizadas, a aferição de gravidade do seu comportamento negligente, terá necessariamente de ter em consideração dois pontos essenciais indissociáveis: o grau de informação que é fornecido ao utilizador por parte do prestador de serviços, no que respeita às operações fraudulentas[254], e bem assim, o grau de diligência do cliente, isto porque, o grau de censura (diligência exigível) que se poderá

[251] Cit. considerando 82 da PRSP- um exemplo de negligência grave seria o utilizador guardar as credenciais utilizadas para autorizar uma operação de pagamento juntamente com o instrumento de pagamento, num formato aberto e facilmente detetável por terceiros; ainda de acordo com o considerando 82 da PRSP, *"o facto de um consumidor já ter recebido um reembolso por parte de um prestador de serviços de pagamento depois de ter sido vítima de fraude por usurpação da identidade de um empregado bancário e de apresentar outro pedido de reembolso ao mesmo prestador de serviços de pagamento, depois de ter sido novamente vítima do mesmo tipo de fraude, pode ser considerado uma «negligência grave» uma vez que poderá indicar um elevado grau de descuido por parte do utilizador, que devia ter exercido maior vigilância depois de já ter sido vítima do mesmo modus operandi fraudulento".* Por outro lado, o Acórdão do Supremo Tribunal de Justiça, de 12-12-2023 (Manuel Capelo), "*A negligência grosseira, merecedora de reprovação pelo mais elementar senso comum por configurar uma falta indesculpável na omissão dos deveres a que se está obrigado, não se verifica quando a lesada, com a atenção que lhe era exigida e de que era capaz nas circunstâncias do caso, não se pôde opor aos artifícios de complexidade eletrónica que lhe foram colocados por terceiros que se fizeram passar com aparente credibilidade pelos serviços do banco, solicitando a resolução de um problema que efetivamente, em momento anterior e por duas vezes, o banco informara dever ser resolvido*", considerando assim não existir negligência grosseira na atuação de um utilizador de um serviço de *homebanking* que, em resposta à solicitação feita por uma SMS, identificada como proveniente do banco, acede a um *website* ali indicado, em tudo igual à página oficial do Banco, usando para isso o seu número de utilizador e PIN e fornecendo também os números do seu cartão matriz, com a finalidade de ativar o serviço que estava inativo, conforme por duas vezes o banco anteriormente informara.

[252] Assim o Acórdão do Tribunal da Relação do Porto de 19-12-2023, (Paulo Duarte Teixeira).

[253] Inocêncio Galvão Teles, *in Direito das Obrigações*, 5.ª Ed., pp. 325-326. Também sobre a distinção entre culpa grave e culpa leve, *vide,* António Menezes Cordeiro, *Tratado de Direito Civil, VIII*, 2ª Edição Revista e Atualizada, Coimbra, Almedina, 2023 e Menezes Leitão, em *Direito das Obrigações,* cit., pp. 311-313.

[254] A este respeito, Maria Raquel Guimarães, "Pagamentos electrónicos não autorizados e fraudulentos", cit., pp. 227-240.

imputar ao cliente, deverá estar em linha com o nível de esclarecimento e de informação que o prestador de serviços de pagamento proporciona ao seu cliente[255].

Conforme já tivemos oportunidade de referir em sede anterior, a PRSP, à semelhança da DSP2, faz pender sobre o prestador de serviços de pagamento um conjunto de regras de controlo de riscos operacionais e de comunicação de fraudes[256]. Na mesma linha, a PRSP consagra agora os deveres de informação e esclarecimento a prestar ao utilizador, que devem ser garantidos pelo prestador de serviços de pagamento[257].

A verdade é que tem sido já comum na jurisprudência nacional convocar a responsabilidade do banco, pela falta de informação prestada ao utilizador, ilidindo assim a culpa deste último[258]. A este respeito, equacione-se um cenário de *phishing*, em que utilizador de serviço de pagamento fornece as suas credenciais associadas a um instrumento de pagamento, bem como, o acesso aos elementos de autenticação forte, em resposta a um *email* ou SMS fraudulento. O grau de censura ao comportamento do utilizador não poderá ser alheio à informação fornecida pelo prestador de serviços de pagamento ao utilizador, havendo de se fazer uma necessária distinção entre a atuação de um utilizador que já havia sido alertado pelo banco, daquele que nunca foi alertado para a possibilidade de ser vítima de fraude por via de SMS e *emails* fraudulentos[259]. Quer isto também dizer que importará aferir os termos em que o utilizador de serviços de pagamento procede à transmissão dos seus dados a terceiros, na medida em que esse circunstancialismo será relevante para apurar o grau de censura a imputar ao comportamento do cliente[260]. O critério de diligência do agente deverá ser determinado pelo

---

[255] Maria Raquel Guimarães, "«Na minha Conta ou na tua?»…", cit., p. 79.
[256] Artigos 81.º e 82.º da PRSP e artigos 95.º e 96.º da DSP2.
[257] Artigo 84.º da PRSP.
[258] Veja-se o Acórdão do Tribunal da Relação de Coimbra, de 15-01-2019 (Moreira do Carmo), em que o utilizador, confiando encontrar-se na página fidedigna do Banco, introduziu os dados ali solicitados, sem que se apercebesse que se tratava de uma página fraudulenta (*pharming*), o Tribunal, para apuramento do grau da eventual negligência grosseira do Cliente, considerou que da *"factualidade apurada nos autos, como dos elementos documentais de que se dispõe, não se retira que o Banco tivesse comunicado ao autor regras, conselhos ou advertências específicas para a utilização do "homebanking", tendo apenas ficado demonstrado que o autor ficou elucidado acerca dos procedimentos a adoptar para concretizar as operações bancárias que pretendesse realizar"* tendo por esta via considerado que o cliente não agiu com negligência grave. Em sentido oposto, o Acórdão de Relação de Évora, 12-04-2018 (Ana Margarida Lebre), dispõe que "*A advertência, que fora transmitida ao autor e que constava do cartão matriz, de que a solicitação de mais de duas posições desse cartão indicia a presença de página fraudulenta, impunha cautela ao autor, permitindo-lhe prever a possibilidade de não se encontrar no sítio eletrónico correto e de estar a facultar os seus dados a terceiros*", julgando que a atuação do Cliente, ao inserir a totalidade das coordenadas inscritas no cartão matriz numa página eletrónica semelhante à do serviço de *homebanking* do Banco, configura negligência grave.
[259] Neste sentido, Maria Raquel Guimarães, "«Na minha Conta ou na tua?»…", cit., p. 83.
[260] *Cfr.* Francisco Mendes Correia, em "Operações não autorizadas e o Regime jurídico dos serviços de pagamento e da moeda eletrónica", cit., p. 717; no mesmo sentido o Autor, em "Responsabilidade e Risco nas operações de pagamentos não autorizadas", cit., p. 444; e bem assim, o Acórdão da Relação de Lisboa de 15-03-2016 (Rijo Ferreira), segundo o qual: "*pela própria natureza das coisas, (não) se pode qualificar a conduta de quem fornece credenciais de segurança sujeito a uma prática fraudulenta('phishing','pharming','keylogging')como*

padrão de diligência objetivo do *bonus pater familias*[261]. Na graduação da culpabilidade do ordenante, há que ter em conta "os valores ou interesses que se pretendem acautelar com o comportamento devido, bem como, a intervenção da vontade na omissão de tal comportamento"[262], considerando-se todas as circunstâncias concretas do caso, à luz de critérios de razoabilidade[263].

4.2. ÓNUS DA PROVA NAS OPERAÇÕES NÃO AUTORIZADAS

No que concerne ao ónus da prova nas operações não autorizadas, a PRPS também não consagra novidades face à DSP2. Perante a comunicação de uma operação não autorizada, cabe ao prestador de serviços de pagamento fazer prova de que a operação foi devidamente autorizada, registada, e contabilizada, bem como, provar que a operação em questão não foi alvo de qualquer avaria técnica ou qualquer outra deficiência do serviço prestado[264]. Esse ónus passará a recair sobre o prestador de serviços de iniciação de pagamento, dentro da esfera das suas competências, quando uma operação seja iniciada através do seu serviço. Assim, cabe ao prestador de serviços de pagamento ou ao prestador de serviços de iniciação de pagamento, fazer prova de elementos que demonstrem a existência de fraude ou negligência grave por parte do utilizador do serviço de pagamento[265], não sendo bastante para provar a autorização da operação de pagamento a simples a demonstração da utilização do instrumento de pagamento registada pelo prestador do serviço de pagamento ou pelo prestador do serviço de iniciação de pagamento[266], ou seja, a prova necessária terá de ser alicerçada em juízos de ilicitude e censura do comportamento do cliente[267].

---

gravemente negligente (..) e para uma conduta poder qualificada como grosseiramente negligente ela não pode ser susceptível de ser levada a cabo por um número significativo dos homens médios"; no mesmo sentido o Acórdão da Relação de Coimbra de 15-01-2019 (Moreira do Carmo).

[261] Francisco Mendes Correia, "Responsabilidade e Risco nas operações de pagamentos não autorizadas", cit., p. 445. Neste sentido, o Acórdão da Relação de Coimbra, de 10-12-2020 (Emídio Santos): "*a negligência assenta na comparação entre a conduta concreta, provada, do agente e uma conduta hipotética que tem por referência a diligência de um bom pai de família, em face das circunstâncias de cada caso*".

[262] Acórdão de Relação de Évora, 12-04-2018 (Ana Margarida Lebre), cit.

[263] Neste sentido, Francisco Mendes Correia, "Responsabilidade e Risco nas operações de pagamentos não autorizadas", cit., p. 446, em conformidade com as decisões que vêm sido proferidas pela Jurisprudência nacional. Nas palavras de Maria Raquel Guimarães, a "*actuação gravemente negligente do utilizador de um instrumento de pagamento pressupõe que este adopta um comportamento que um utilizador médio, razoavelmente informado e esclarecido, não adoptaria*", em "«Na minha Conta ou na tua?»…", cit., p. 84

[264] Artigo 55.º, n.º 1 da PRSP e artigo 72.º, n.º 2 da DSP2.

[265] Artigo 55.º, nº. 2 e artigo 72.º, n.º 2.

[266] Francisco Mendes Correia, em "Responsabilidade e Risco nas operações de pagamentos não autorizadas", cit., p. 463. De sublinhar que isto não significa dizer que a prova da utilização do instrumento de pagamento não será relevante para efeitos probatórios, quando conjugada com outros fatores – *cfr.* sustenta Maria Raquel Guimarães, em "As operações fraudulentas de *homebanking* na jurisprudência recente: Acórdão do Supremo Tribunal de Justiça de 18/12/2013, Proc. 6479/09", p. 31.

[267] Idem, p. 464.

Conforme começamos por referir, a PRSP não apresenta alterações face ao regime consagrado na DSP2, com uma pequena ressalva para o facto de o primeiro normativo se referir à "prova de que a operação de pagamento foi autorizada", ao passo que a DSP2 faz referência a "autenticação" ao invés de "autorização", ou seja, lança mão de um critério mais alargado. Não parece, no entanto, ser uma alteração com relevância na concreta aplicação do regime em causa, até porque, a referência a "prova da autorização" é também feita no âmbito do normativo em vigor, traduzindo-se apenas numa questão de semântica.

O regime do ónus da prova consagrado é um elemento crucial no que respeita à tutela da posição "débil" do utilizador face ao prestador de serviços de pagamento[268], sobre o qual recai, conforme tem sido amplamente repetido, a obrigação de assumir uma posição proactiva, de adoção de mecanismos eficazes de prevenção e combate à fraude. A aplicação deste regime não tem levantado dúvidas no âmbito da jurisprudência nacional, sendo de pacífica aceitação, entendimento e aplicação[269].

É de sublinhar ainda a especial preocupação do legislador com o utilizador-consumidor, na medida que, embora preveja a possibilidade de as regras referentes ao ónus da prova poderem ser afastadas por acordo entre as partes, essa possibilidade apenas é concedida aos utilizadores não consumidores[270], uma vez que, no entendimento do legislador, consumidores e empresas não se encontram na mesma situação de vulnerabilidade, não sendo necessário garantir o mesmo nível de proteção[271].

4.3. OPERAÇÕES AUTORIZADAS

Nos últimos anos, conforme já referido anteriormente, os números de casos de "engenharia social" têm vindo a aumentar. Estas situações têm vindo a ocorrer através de múltiplos canais, incluindo *email*, SMS, telefonemas e redes sociais, numa tentativa de obterem as credenciais

[268] A este respeito, Hugo Luz dos Santos, em "Plaidoyer por uma "distribuição dinâmica do ónus da prova" e pela "teoria das esferas de risco" à luz do recente acórdão do Supremo Tribunal de Justiça, de 18/12/2013: o (admirável) "mundo novo" no homebanking?"*, in Revista Electrónica de Direito*, Abril de 2014, pp. 21 e s.s.; e também Patrícia Guerra, em "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", cit., p. 26.

[269] Neste sentido, o Acórdão do Tribunal da Relação de Lisboa, de 28-04-2022, Relator Luís Correia de Mendonça, "*De acordo com esse regime, cabe ao prestador do serviço de transferência, provar não só que a operação de pagamento foi autenticada, devidamente registada e contabilizada, mas também que a operação não foi afectada por avaria técnica ou qualquer outra deficiência*; também no mesmo sentido o Acórdão do Tribunal da Relação do Porto, de 27-06-2022, (Mendes Coelho); bem assim, Acórdão da Relação do Porto, de 12-10-2023 (Ana Luísa Loureiro); e ainda Acórdão do Supremo Tribunal de Justiça, de 23-01-2024, (Nelson Borges Carneiro).

[270] Artigo 27.º, n.º 1 da PRSP e artigo 61.º, n.º 1 da DSP2; mais, de acordo com o Considerando 83 da PRSP, devem ser considerados nulos os termos e condições contratuais relativos ao fornecimento e à utilização de um instrumento de pagamento que tenham por efeito agravar o ónus da prova que recai sobre o consumidor ou atenuar o ónus da prova que recai sobre o emitente.

[271] Considerando 39 da PRSP. Já assim o entendia no âmbito da DSP2, *cfr.* Considerando53 daquela Diretiva.

de acesso do utilizador a um serviço de pagamento, ou mesmo o acesso direto ao serviço[272]. São muitos os casos em que ocorre a usurpação de identidade do prestador do serviço de pagamento. Os agentes fraudulentos fazem-se passar por empregados do prestador de serviços de pagamento e utilizam, abusivamente, o nome, o endereço de correio eletrónico ou o número de telefone do prestador de serviços de pagamento para ganhar a confiança do cliente em questão, de modo a convencê-lo a executar determinadas ações[273]. Ora, este tipo de fraude, que recorre à usurpação de identidade, está a esbater as diferenças entre operações autorizadas e não autorizadas[274]. O que acontece, não raras vezes, é que o agente fraudulento assume o controlo de todo o processo de autorização e autenticação no âmbito da operação bancária, substituindo-se ao cliente. A operação é, de facto, autorizada, mas não (pelo menos, de forma consciente) pelo cliente. Atento a esta problemática, o legislador percebeu, e bem, que a proteção do utilizador dos serviços de pagamento não se poderia esgotar no âmbito das operações não autorizadas, conforme se verifica no atual enquadramento jurídico conferido pela Diretiva (UE) 2015/2366, devendo sim, abranger também casos de pagamentos autorizados pelo cliente[275]. Para o efeito, importa aferir as concretas circunstâncias em que foi concedida a autorização e efetuada a autenticação forte do cliente no âmbito de uma operação de pagamento[276], designadamente, se houve manipulação do utilizador por parte de um agente terceiro, que, de algum modo, se fez passar por agente associado ao prestador de serviços de pagamento.

Este é de facto um importante acrescento que a PRSP vem fazer ao quadro regulamentar dos serviços de pagamentos, com vista a conferir maior tutela aos consumidores[277]. Assim, a proposta apresentada pelo legislador europeu, prevê que os consumidores terão direito ao

[272] Neste sentido, Maria Raquel Guimarães, "Mb way, 'engenharia social' e operações fraudulentas", *cit.*.
[273] Analisada a Jurisprudência nacional, são inúmeros os casos em que verifica a usurpação da identidade do banco. Veja-se por exemplo: Acórdão do Tribunal da Relação de Lisboa, de 29-09-2022 (Maria de Deus Correia), em que as credenciais de acesso ao serviço de *homebanking* foram solicitadas através de SMS, em tudo semelhantes às *SMS´s* habitualmente remetidas pelo banco; Acórdão do Tribunal da Relação de Lisboa, de 12-07-2018 (Higina Castelo), em que o cliente procedeu à introdução dos seus dados de autenticação forte, numa página *web* semelhante à página do banco, na qual chegou ao clicar numa hiperligação de um *email*; Acórdão do Tribunal da Relação do Porto, de 16-05-2023 (Rodrigues Pires), em que o cliente forneceu os seus dados confidenciais na sequência do recebimento de um *SMS*, que tudo indicava ser proveniente da respetiva entidade bancária; e ainda, Acórdão do Supremo Tribunal de Justiça, de 12-12-2023, (Manuel Capelo), em que o cliente em resposta à solicitação feita por uma *SMS*, identificada como proveniente de banco prestador do serviço, acede a um *website* ali indicado, semelhante à página do banco, onde fornece o seu número de utilizador e *PIN*, bem como, os números do seu cartão matriz.
[274] *Vide* considerando 79 da PRSP.
[275] Artigo 59.º da PRSP. Sobre esta temática, ver Maria Raquel Guimarães, "«Na minha Conta ou na tua?»…", cit., pp. 103-105.
[276] *Cfr.* considerando 79 da PRSP.
[277] De sublinhar que a lei faz expressa referência à qualidade de consumidor, fazendo crer que esta tutela apenas recai sobre os clientes-consumidores.

reembolso do montante integral da operação de pagamento fraudulenta, sempre que a autorização tenha por base a manipulação do utilizador por um terceiro que se faça passar por um empregado do prestador de serviços de pagamento[278], utilizando, indevidamente, o nome, o endereço de correio eletrónico ou número de telefone desse prestador de serviço de pagamento. Sublinhe-se que, como condição para o reembolso, é exigida a comunicação, sem demora, da operação de pagamento fraudulenta, às autoridades policiais e ao respetivo prestador de serviço de pagamento, sendo que, se esses trâmites processuais forem preteridos, não deve ser concedido qualquer reembolso[279]. Em tudo o resto, o legislador equipara as regras do reembolso às previstas no âmbito das operações não autorizadas: o reembolso deve ocorrer no prazo de 10 dias, ou deve o prestador de serviço de pagamento apresentar causa justificativa para a recusa do mesmo, munido de prova bastante que ateste a atuação fraudulenta ou com negligência grave do cliente[280].

Sucede que, as fraudes com recurso a mecanismos de "engenharia social" não se esgotam na usurpação de identidade de um empregado do prestador de serviço de pagamento. As operações fraudulentas ocorrem também através de plataformas como o *WhatsApp*, SMS, mensagens de voz e redes sociais, em que, regra geral, o agente fraudulento faz-se passar por um ente querido da vítima, alegando estar numa situação de dificuldade, solicitando uma transferência de fundos a seu favor[281]. São esquemas que, maioritariamente, assentam em técnicas de persuasão, através da criação de narrativas credíveis para convencer as vítimas a realizar as transferências solicitadas. Do mesmo modo, o aumento do comércio eletrónico entre particulares, em plataformas como o OLX e outros *marketplaces*, tem sido gerador de diversas situações de fraude, em que, o desconhecimento do modo de utilização de aplicações de pagamento, como o *MB Way*, leva a que a vítima seja conduzida pelo agente fraudulento a

[278] O Parlamento Europeu propõe alterações ao texto do artigo 59.º, n.º 1 da PRSP, alargando o âmbito desta norma aos casos em que um terceiro se faça passar por um empregado de "*qualquer outra entidade relevante de natureza pública ou privada*". Acrescenta a necessidade de serem aplicadas medidas educativas sobre formas de identificar situações de fraude, bem como, medidas preventivas de combate à fraude. Propõe ainda que, 12 meses após a entrada em vigor da PRSP, a EBA deve emitir orientações técnicas no que respeita ao conceito de «negligência grave» no contexto do Regulamento. Por seu turno, o Banco Central Europeu entende que o regime proposto se destina unicamente a regular casos complexos e sofisticados de fraude, em que nenhum nível de educação ou diligência dos clientes seriam suficientes para detetar a fraude, e não abrange outros tipos de usurpação de identidade, para além da usurpação de identidade bancária, *cfr. Parecer do Banco Central Europeu CON/2024/13)*.
[279] *Cfr.* considerando 80 da PRSP.
[280] Artigo 59.º, n.ºs 2, 3 e 4 da PRSP.
[281] A este respeito, refira-se o famoso esquema "Olá mãe, olá pai", amplamente difundido nos *media* nacionais, em que um terceiro, que se apresenta como sendo o seu filho ou outro familiar próximo da vítima, alega estar a usar o telemóvel de um amigo porque perdeu o seu, ou porque avariou, solicitando uma transferência de fundos urgente para a aquisição de novo telemóvel.

promover um pagamento, quando na verdade julga estar a introduzir credenciais para um recebimento, e bem assim, não raras vezes, está mesmo a facultar o acesso à sua conta[282].

Não obstante todo o exposto, o legislador europeu considerou que seria "desproporcionado e financeiramente muito oneroso para os prestadores de serviços de pagamento"[283] sujeitar todas as operações fraudulentas, autorizadas ou não, a um direito de reembolso sistemático. Nesta medida, haverá que aferir se estamos perante operações de pagamento (validamente) autorizadas pelo utilizador – que em regra não serão reembolsáveis, ou, perante operações de pagamento não autorizadas. A dificuldade reside precisamente em aferir as condições em que o cliente deu a sua autorização a uma operação, cabendo ao prestador de serviço de pagamento, em último *ratio*, fazer prova da autorização de pagamento efetuada pelo utilizador, conforme as regras relativas aos ónus da prova previstas na DSP2 e na PRSP[284]. Nesta medida, antevê-se que provenha daqui alguma dificuldade futura para os tribunais nacionais, na concreta destrinça entre as operações autorizadas e não autorizadas[285].

Ainda no âmbito das operações autorizadas, e atenta a nova disposição relativa à responsabilidade pela incorreta aplicação do serviço de verificação de correspondência de IBAN e nome do beneficiário[286], cumpre fazer referência à imputação da responsabilidade pelos prejuízos ao PSP do ordenante[287] (pelo montante total da transferência), sempre que haja incumprimento do dever comunicação/notificação da discrepância detetada entre o identificador único e o nome do beneficiário fornecido pelo ordenante, e sempre que este não tenha atuado de forma fraudulenta ou com negligência grave[288]. Diferente será, quando, após ter tomado conhecimento da discrepância detetada, ainda assim, o ordenante autorizar a transferência a crédito, cenário em que, estando em causa uma operação autorizada, a responsabilidade pelas perdas correrá por sua conta[289].

---

[282] Para melhor entendimento desta temática, Maria Raquel Guimarães, "*Mb way*, 'engenharia social' e operações fraudulentas", *cit.*.

[283] Considerando 79 da PRSP.

[284] Também neste sentido, Maria Raquel Guimarães, "«Na minha Conta ou na tua?»…", cit., p. 105.

[285] Ainda conforme o considerando 79 da PRSP.

[286] Artigo 57.º da PRSP.

[287] Sem prejuízo do direito de regresso sobre o prestador de serviços de pagamento do beneficiário, se a este for imputável o incumprimento desta comunicação, *cfr.* o artigo 57.º, n.º 1, e o considerando 78 da PRSP.

[288] Artigo 67.º, n.º 3 da PRSP. Sobre este tema, Maria Raquel Guimarães, "«Na minha Conta ou na tua?»…", cit., p. 111. Remetemos também para os desenvolvimentos que tecemos, *supra*, sobre este tema.

[289] Na eventualidade de a falta de notificação da discrepância se dever a uma falha do prestador de serviços de pagamento do beneficiário, terá o prestador de serviços de pagamento do utilizador direito de regresso sobre aquele, c*fr.* n.º 3 do artigo 50.º da PRSP.

5. CONCLUSÃO

No presente trabalho de dissertação propusemo-nos a analisar o futuro dos serviços de pagamento, à luz da nova proposta de Regulamento. Aqui chegados, cumpre fazer um balanço sobre os impactos expectáveis face às alterações legislativas propostas pela Comissão.

Ora, dúvidas não restam que a implementação do novo RSP terá impacto no panorama dos serviços de pagamento na Europa, representando mais um passo para o setor dos serviços financeiros, com vista a acompanhar a constante transformação digital, sem deixar de priorizar os interesses, a segurança e a confiança dos consumidores.

Conforme tivemos oportunidade de analisar, a Comissão Europeia vem apresentar uma revisão significativa do quadro legal dos serviços de pagamento, com foco principal nas temáticas identificadas no relatório de avaliação *ex post* da DSP2. Com as presentes alterações legislativas espera-se uma melhoria no âmbito da proteção e confiança dos consumidores, de modo a incentivar uma maior utilização dos serviços de pagamento eletrónico; colocar cobro aos obstáculos que têm obstado ao pleno funcionamento do *open banking*, com vista a garantir condições de concorrência entre os bancos e os prestadores de serviços de pagamento não bancários; bem como, procurar uma maior harmonização legislativa entre os diferentes Estados-Membros.

Da análise comparativa entre o regime da DSP2 e a proposta de Regulamento apresentada, concluímos que o legislador não efetuou alterações substanciais, antes sim, procurou maior concretização, balizando as exceções, clarificando conceitos e atribuindo maior autoridade às entidades competentes pela concreta fiscalização da execução normativa.

Cumpre começar por louvar a opção disruptiva no que concerne ao instrumento escolhido - Regulamento. O facto de ser diretamente aplicável a todos o Estados-Membros, dispensando-se atos legislativos nacionais de transposição para as ordens jurídicas, espera-se, conduzirá a maior harmonização legislativa nos diferentes Estados-Membros. O legislador pretende assim colocar cobro às aplicações e interpretações divergentes em toda a UE. Parece-nos ser uma resposta assertiva e inovadora, com vista à plenitude do Mercado Único.

Por outro lado, o quadro normativo agora proposto espelha também a preocupação do legislador em promover a concorrência e em garantir o pleno funcionamento do *open banking*, que ajudará a impulsionar a inovação e a entrada de novos intervenientes no mercado, o que só poderá ser benéfico para os consumidores, oferecendo-lhes uma maior variedade de opções e serviços mais personalizados.

No que respeita à responsabilidade por operações de pagamentos não autorizadas, os provedores de serviços de pagamento passam a ser responsabilizados num maior número de

situações, e serão obrigados a tomar medidas adicionais de combate à fraude, através de ações de sensibilização dos consumidores, bem como, através da partilha de informação sobre fraude entre os diferentes prestadores de serviços de pagamento. O legislador visa assim dar um passo em frente no combate à fraude.

É de referir que, as alterações agora propostas impõem importantes desafios para os bancos e instituições financeiras tradicionais, na medida em que terão de se adaptar às novas exigências e competir com *fintechs* e prestadores de serviços de pagamento não tradicionais.

Embora as propostas legislativas analisadas ainda estejam sujeitas a alterações e discussões, é desde já evidente que terão um impacto significativo no panorama dos serviços de pagamento na Europa. Na presente data, foram já emitidos diversos pareceres sobre a PRSP, nomeadamente, parecer do Comité Económico e Social Europeu[290], parecer da Comissão dos Assuntos Económicos e Monetários[291], e parecer do Banco Central Europeu[292]. O Parlamento Europeu apresentou já, em sede de primeira leitura em processo legislativo ordinário, proposta de alteração à proposta de RSP apresentada pela Comissão[293], alterações que recaem essencialmente sobre matérias de transparência na informação a prestar aos utilizadores, reforço das medidas de proteção dos PSP's não bancários, bem como, reforço de algumas medidas no âmbito da proteção dos utilizadores. Não obstante, aguarda-se ainda pela posição do Conselho em primeira leitura, até que seja conhecida a proposta legislativa final a adotar.

Existindo ainda um longo caminho até à publicação e entrada em vigor do quadro legal analisado, não são expectáveis mudanças significativas. Espera-se que a versão final seja publicada até ao final do presente ano (2024), seguindo-se o procedimento legislativo habitual, sendo expectável que a DSP3 e o RSP entrem em vigor em meados de 2026.

---

[290] Parecer do Comité Económico e Social Europeu, C/2024/1594, de 5.3.2024, disponível em <C_202401594PT.000101.fmx.xml (europa.eu)> (16-07-2024).

[291] Relatório sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo aos serviços de pagamento no mercado interno e que altera o Regulamento (UE) n.º 1093/2010, 22.2.2024 - (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)), Comissão dos Assuntos Económicos e Monetários, disponível em <REPORT on the proposal for a regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 | A9-0052/2024 | European Parliament (europa.eu)> (23-07-2024)

[292] Parecer do Banco Central Europeu de 30 de abril de 2024 sobre uma proposta de Regulamento e de Diretiva relativa aos serviços de pagamento e de moeda eletrónica, (CON/2024/13), C/2024/3869 de 19.6.2024, disponível em < C_202403869PT.000101.fmx.xml (europa.eu)> (16-07-2024).

[293] Resolução legislativa do Parlamento Europeu, de 23 de abril de 2024, sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo aos serviços de pagamento no mercado interno e que altera o Regulamento (UE) n.º 1093/2010 (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD), disponível em <TA (europa.eu)> (16-07-2024).

BIBLIOGRAFIA

ACEPI — Associação Portuguesa da Economia Digital, *Economia digital em Portugal – Edição 2022*, pp. 37-41, disponível em <Estudo-da-Economia-e-da-Sociedade-Digital-2022-ACEPI-IDC-PT-Versão-Completa.pdf (computerworld.com.pt)>(11-06-2024)

ANACOM — Autoridade nacional de comunicações, *O comércio eletrónico em Portugal e na União Europeia- Segmento residencial e empresarial- Relatório de 2021*, disponível em <ComercioEletronico2021_final.pdf (anacom.pt)> (26-05-2024)

Antunes, José Engrácia, *Direito dos Contratos Comerciais*, Almedina, Coimbra, 2009

Autoridade Bancária Europeia (EBA), *Strong customer authentication and common and secure communication (incl. access)*, *Q&A 2018_4058,* de 01 de março de 2019, disponível em < 2018_4058 Transactions initiated via Interactive Voice Response (IVR) solutions | European Banking Authority (europa.eu)> (26-05-2024)

Autoridade Bancária Europeia (EBA), *Aplicabilidade do SCA a 'pagamentos por cartão iniciados apenas pelo beneficiário*, Q&A 2018_4031, de 01 de março de 2019, disponível em <2018_4031 Applicability of SCA to 'card payments initiated by the payee only' | European Banking Authority (europa.eu)> (26-05-2024).

Autoridade Bancária Europeia (EBA), *Clarification on whether a particular business model type constitutes the provision of an account information service as defined by Article 4 (16) of PSD2*, Q&A 2018_4098, de 13 de setembro de 2019, disponível em: <2018_4098 Clarification on whether a particular business model type constitutes the provision of an account information service as defined by Article 4 (16) of PSD2 | European Banking Authority (europa.eu)> (26-05-2024).

Autoridade Bancária Europeia (EBA), *Guidelines on the limited network exclusion under PSD2*, (EBA/GL/2022/02), 24 de fevereiro de 2022, disponível em <Final report on draft Guidelines on the limited network exclusion under PSD2.pdf (europa.eu)> (26-05-2024)

Autoridade Bancária Europeia (EBA), *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, (EBA/Op/2022/06), de 23 de junho de 2022, disponível em <EBA's response to the Call for advice on the review of PSD2.pdf (europa.eu)> (26-05-2024)

Autoridade Bancária Europeia (EBA), *Opinion of the European Banking Authority on "de-risking"*, (EBA/Op/2022/01) 5 de janeiro de 2022, disponível em <EBA Opinion and annexed report on de-risking.pdf (europa.eu)>(26-05-2024)

Autoridade Bancária Europeia (EBA), *Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC*, (EBA/OP/2020/10), 4 de junho de 2020, disponível em <EBA Opinion on obstacles under Art. 32(3) RTS on SCA&CSC.pdf (europa.eu)> (26-05-2024)

Autoridade Bancária Europeia (EBA), *Strong customer authentication and common and secure communication (incl. access), Q&A 2019_4788*, de 12 de março de 2021, disponível em <2019_4788 Treatment of electronic bookings similar to Mail Order and Telephone Orders (MO-TO) transactions | European Banking Authority (europa.eu) > (26-05-2024)

Autoridade Bancária Europeia (EBA), *Strong customer authentication and common and secure communication (incl. access), Q&A 2019_4790*, de 12 de março de 201, disponível em <2019_4790 Keyed Mail Order or Telephone Order (MO-TO) transactions | European Banking Authority (europa.eu)> (26-05-2024)

Banco Central Europeu, *Parecer do Banco Central Europeu de 30 de abril de 2024 sobre uma proposta de Regulamento e de Diretiva relativa aos serviços de pagamento e de moeda eletrónica*,(CON/2024/13), C/2024/3869 de 19.6.2024, disponível em < C_202403869PT.000101.fmx.xml (europa.eu)> (16-07-2024)

Banco de Portugal, *Audição da Comissão de Orçamento, Finanças e Modernização Administrativa (COFMA) - Diretiva dos serviços de pagamento revista (DSP2)*, 15 de Junho de 2018, disponível em <Apresentação do Diretor do Departamento de Serviços Jurídicos, Pedro Machado, e do Diretor do Departamento de Sistemas de Pagamentos, Egrejas Francisco na Comissão de Orçamento, Finanças e Modernização Administrativa sobre Serviços de Pagamento de Moeda Eletrónica (bportugal.pt)> (26-05-2024)

Banco de Portugal, *Diretiva dos Serviços de Pagamentos revista (DSP2) foi transposta para o ordenamento jurídico nacional. O que muda?*, disponível em <Diretiva dos Serviços de Pagamentos revista (DSP2) foi transposta para o ordenamento jurídico nacional. O que muda? | Banco de Portugal (bportugal.pt)> (26-05-2024)

Banco de Portugal, *Fintech +, o novo canal do Banco de Portugal sobre inovação financeira*, de 23-05-2018, disponível em <Fintech +, o novo canal do Banco de Portugal sobre inovação financeira | Banco de Portugal (bportugal.pt)> (26-05-2024)

Banco de Portugal, *Relatório dos Sistemas de Pagamentos — 2022,* Lisboa, 2023, disponível em <Relatório dos Sistemas de Pagamentos 2022 (bportugal.pt)> (26-04-2024)

Banco de Portugal, *Relatório dos Sistemas de Pagamentos — 2023,* Lisboa, 2024, disponível em <Relatório dos Sistemas de Pagamentos - 2023 (bportugal.pt)> (09-06-2024)

Barbosa, Mafalda Miranda, "Serviços de pagamentos, repartição do risco e responsabilidade civil – algumas reflexões a propósito da nova diretiva dos serviços de pagamentos (DSP2)", *in Revista de Direito Comercial*, 2017, pp. 622-682

Berga, Toni; *Del 'open banking' de PSD2 al 'open finance' de PSD3*, de 01-02-2023, disponível em <Del 'open banking' de PSD2 al 'open finance' de PSD3 | Embat> (04-06-2024)

Bianco, Sébastien, *How do PSD3 and PSR impact the EU payments sector?,* de 19-04-2024, disponível em <How do PSD3 and PSR impact the EU payments sector? - Powens> (20-07-2024)

Bindseil, Ulrich; Hempel, Monika, "A estratégia do Eurosistema para os pagamentos de retalhoThe Eurosystem retail payments strategy", *in InforBANCA- Revista do Instituto de Formação Bancária*, edição nº 121, janeiro 2021, pp. 11 a 16, disponível em < IFB-InforBanca-121_JAN2021.pdf > (11-06-2024)

Cavaco, Maria Tereza, "Pagamentos: o futuro já começou"*, in InforBANCA- Revista do Instituto de Formação Bancária,* edição nº 130, janeiro 2024, pp. 16 a 20, disponível em <InforBanca-130-JANEIRO-2024.pdf (ifb.pt)> (11-06-2024)

Chaney, Laura; Renda, Vicenzo, "How to Design a Successful European Payments Market? DIGITALEUROPE's position on the Payment Services Regulation (PSR) and Payment Services Directive 3 (PSD3) Proposals" *in Digital Europe*, 17-11-2023, disponível em <Payment-Services-Regulation-PSR-position-paper.pdf (digitaleurope.org)> (26-05-2024)

Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre uma Estratégia em matéria de Financiamento Digital para a EU*, COM (2020) 591 final, Bruxelas, 24.9.2020

Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre uma Estratégia para os pagamentos de pequeno montante na EU*, COM (2020) 592 final, Bruxelas, 24.9.2020

Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre uma Estratégia em matéria de Financiamento Digital para a EU*, COM(2018) 109 final, Bruxelas, 8.3.2018;

Comissão Europeia, *Consultation on a retail payments strategy for the EU*, disponível em <2020 - Retail payments strategy - European Commission (europa.eu)> (24-06-2024)

Comissão Europeia, *Convite à apreciação de uma avaliação e de uma avaliação de impacto realizadas em paralelo*, Ref. Ares(2022)3556263, de 10/05/2022, disponível em <Serviços de pagamento — revisão das normas da UE (europa.eu)> (26-05-2024)

Comissão Europeia, *Modernizar os serviços de pagamento e abrir os dados relativos aos serviços financeiros: novas oportunidades para os consumidores e as empresas*, de 28 de Junho de 2023, Bruxelas, disponível em <Modernizar os serviços de pagamento e os dados relativos aos (europa.eu)> (06-06-2024)

Comissão Europeia, *Proposta de Diretiva do Parlamento Europeu e do Conselho relativa aos serviços de pagamento e aos serviços de moeda eletrónica no mercado interno que altera a Diretiva 98/26/CE e revoga as Diretivas (UE) 2015/2366 e 2009/110/CE*, COM(2023) 366 final, Bruxelas, 28.6.2023.

Comissão Europeia, *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo aos serviços de pagamento no mercado interno e que altera o Regulamento (UE) n.º 1093/2010*, COM(2023) 367 final Bruxelas, 28.6.2023.

Comissão Europeia, *Relatório da Comissão ao Parlamento Europeu e ao Conselho sobre a avaliação dos riscos de branqueamento de capitais e de financiamento do terrorismo relacionados com atividades transnacionais a que está exposto o mercado interno*, COM (2017) 340 final, Bruxelas, 26.6.2017

Comité Económico e Social Europeu, C/2024/1594 *Parecer do Comité Económico e Social Europeu*, C/2024/1594, de 5.3.2024, disponível em <C_202401594PT.000101.fmx.xml (europa.eu)> (16-07-2024)

Conselho Europeu Conselho da União Europeia, *Finança Digital*, de 04 de março de 2024 disponível em <Finança digital - Consilium (europa.eu)> (24-06-2024)

Cordeiro, Menezes António, *Tratado de Direito Civil, VIII*, 2ª Edição Revista e Atualizada Coimbra, Almedina, 2023

Correia, Francisco Mendes, "Operações não autorizadas e o Regime jurídico dos serviços de pagamento e da moeda eletrónica", *in Revista de Direito Civil*, Ano II (2017), Número 3, Coimbra, Almedina, 2017, pp. 701-727

Correia, Francisco Mendes, "Os novos serviços de iniciação de pagamentos: algumas notas sobre a responsabilidade civil", *in Estudos de direito do consumo*, volume II, Rui Mascarenhas Ataíde, Francisco Rodrigues Rocha, Vítor Palmela Fidalgo (org.), Coimbra, Almedina, 2023, pp. 755-770

Correia, Francisco Mendes, "*Responsabilidade e Risco nas operações de pagamentos não autorizadas*", *in Revista da Faculdade de Direito da Universidade de Lisboa*, 2023, nº2, pp.417-466

Correia, Francisco Mendes, "Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento", *in III Congresso de direito bancário*, Coimbra, Almedina, 2017, pp. 385-404

Correia, Francisco Mendes, *Moeda bancária e cumprimento - O cumprimento das obrigações pecuniárias através de serviços de pagamento,* Coimbra, Almedina, 2017

European Central Bank, *Study on the payment attitudes of consumers in the euro area (SPACE), 2022,* disponível em <Study on the payment attitudes of consumers in the euro area (SPACE) – 2022 (europa.eu)> (26-05-2024)

European Commission, "Commission staff working document, Impact assessment report, accompanying the documents Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 and Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC, SWD(2023) 231 final, Brussels, 28.6.2023, disponível em <EUR-Lex - 52023SC0231 - EN - EUR-Lex (europa.eu)> (19-07-2024)

European Commission, *Proposal for a Regulation of the european parliament and of the council amending Regulations, As regards instant credit transfers in euro (EU) No 260/2012 and (EU) 2021/1230*, COM (2022) 546 final 2022/0341 (COD), Brussels, 26.10.2022;

European Payments Council (EPC183-22), *2022 Payment Threats and Fraud Trends Report*, novembro de 2022, disponível em <2021 Payments Threats and Fraud Trends Report (europeanpaymentscouncil.eu)> (24-06-2024)

Fine, Camden, "Digitalización financiera: el community banking en la era de la disrupción digital", *in Transformación digital y medios de pagouna visión práctica a la luz de la PSD2*, coordinado por Santiago Carbó y Francisco Rodríguez Fernández, Papeles de economía española, N.º 149, 2016. ISSN: 0210-9107, Madrid, pp. 2-20

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", *Revista Electrónica de Direito*, Nº 2, junho 2016;

Guimarães, Maria Raquel, "'Na minha Conta ou na tua?' Revisitação do Regime aplicável às operações fraudulenta à luz da nova Proposta de um Regulamento relativo aos serviços de pagamento no mercado interno, de Junho de 2023", *in A Revista, Supremo Tribunal de Justiça*, 2024, pp. 57-20

Guimarães, Maria Raquel, "A responsabilidade por operações fraudulentas no comércio electrónico", *in Direito e Informação que responsabilidade(s)?*, Ricardo Perlingeiro/Fernanda Ribeiro/Luísa Neto (orgs.), Rio de Janeiro, Editora da UFF, 2013, pp. 259-274, disponível em <Direito e Informação: que responsabilidade(s)? (Law and Information: Reciprocal Liabilities) by Ricardo Perlingeiro, Fernanda Ribeiro, Luísa Neto :: SSRN> (26-05-2024)

Guimarães, Maria Raquel, "La Directiva (ue) 2015/2366, sobre servicios de pago (DSP2) y los pagos electrónicos", Working paper 3/2022, disponível em <Càtedra Jean Monnet de Dret Privat Europeu (ub.edu)> (26-05-2024)

Guimarães, Maria Raquel, "Mb way, 'engenharia social' e operações fraudulentas", *in Nova Consumer Lab,* 31 de maio de 2021, disponível em <MB Way, "engenharia social" e operações fraudulentas (unl.pt)> (26-05-2024)

Guimarães, Maria Raquel, "Pagamentos electrónicos não autorizados e fraudulentos", in *Cibercriminalidade: novos desafios, ofensas e soluções*, PACTOR - Edições de Ciências Sociais, Forenses e da Educação, 2021, pp. 227-240

Guimarães, Maria Raquel, "Serviços de pagamento e instrumentos de pagamento: evoluções recentes", *in Estudos de direito do consumo*, volume II, Rui Mascarenhas Ataíde, Francisco Rodrigues Rocha, Vítor Palmela Fidalgo (org.), Coimbra, Almedina, 2023, pp. 737-753

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*, 2012, n. º 2

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" / The Transposition of PSD2 and Open Banking*, a cura di/(Edd.) E. Bani, V. De Stasio, A. Sciarrone Alibrandi, Bergamo, Sestante Edizioni, 2021, pp. 141-166

Guimarães, Maria Raquel, *O Contrato-Quadro no Âmbito da Utilização de Meios de Pagamento Electrónicos*, Coimbra, Coimbra Editora, 2011

Guimarães, Maria Raquel; Steennot, Reinhard, "Allocation of liability in case of payment fraud: who bears the risk of innovation? A comparison of Belgian and Portuguese law in the context of PSD2", *in European Review of Private Law*, Volume 30, Issue 1, 2022, pp. 29-72

Herrera, Lucía Alvarado, Autenticación reforzada de cliente y responsabilidad en la segunda directiva de servicios de pago, in Revista de Derecho del Sistema Financiero 5, Março de 2023, pp. 69–112.

Kemp, Simon, *Digital 2023: global overview report*, de 26.04.2023, disponível em <Digital 2023: Global Overview Report — DataReportal – Global Digital Insights> (20-07-2024)

Leitão, Menezes Luís, *Direito das Obrigações*, I, 14.ª ed., Coimbra, Almedina, 2017

Llena, José Manuel Navarro, Del "Pay by Bank" a la PSD3, y viceversa. de*12-07-2024, disponível em* <Del "Pay by Bank" a la PSD3, y viceversa. | (granadablogs.com)> (18-07-2020)

Mezzacapo, Simone, "PSD2, online and mobile payments: what transparency for the future of payments?", *in L'attuazione della seconda direttiva sui servizi di pagamento e "open banking" / The Transposition of PSD2 and Open Banking*, A cura di / (Edd.), E. Bani, V. De Stasio, A. Sciarrone Alibrandi, Bergamo, Sestante Edizioni, 2021, pp. 69-108;

Moura, Carlos – "FinTech e regulação no mercado bancário", *in Fintech: desafios da tecnologia financeira* (coord. António Meneses Cordeiro, Ana Perestrelo de Oliveira & Diogo Pereira Duarte), 2.º ed., Coimbra, Almedina, 2019, pp. 21-32
Nablón, Iván, "La identificación electrónica: redefiniendo las reglas del sector financiero", Papeles de Economía Española, n.º 162, 2019, 162-174.

Parlamento Europeu, P9_TA(2024)0298 Serviços de pagamento no mercado interno e alteração do Regulamento (UE) n.º 1093/2010 - *Resolução legislativa do Parlamento Europeu, de 23 de abril de 2024, sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo aos serviços de pagamento no mercado interno e que altera o Regulamento (UE) n.º 1093/2010* (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD), disponível em <TA (europa.eu)> (16-07-2024)

Pereira, Tiago da Cunha "DSP: Oportunidades e desafios", *in Revista de Direito Financeiro e dos Mercados de Capitais*, Vol. (2019), No.5, 507-524, disponível em <Vol.-1-2019-no.-5-Tiago-da-Cunha-Pereira-DSP2-Oportunidades-e-Desafios.pdf (rdfmc.com)> (05-05-2024)

Pozzolo, Alberto Franco, *PSD2 and the transformation of the business model of payment services providers, in L'attuazione della seconda direttiva sui servizi di pagamento e "open banking" / The Transposition of PSD2 and Open Banking,* A cura di / (Edd.), E. Bani, V. De Stasio, A. Sciarrone Alibrandi, Bergamo, Sestante Edizioni, 2021, pp. 29-42

Ratcliff, Christina; De Bono, Jordan; Martinello, Barbara; "O mercado interno: princípios gerais", em *Fichas temáticas sobre a União Europeia*, Parlamento Europeu, novembro de 2023, disponível em <O mercado interno: princípios gerais | Fichas temáticas sobre a União Europeia | Parlamento Europeu (europa.eu)> (04-05-2024)

Rocha, Francisco Rodrigues, "Débitos directos. aspectos de regime de proteccão do consumidor", *in Estudos de direito do consumo*, volume II, Rui Mascarenhas Ataíde, Francisco Rodrigues Rocha, Vítor Palmela Fidalgo (org.), Coimbra, Almedina, 2023, pp. 773-885

Rodrigues, Marta Graça; Silva, Tomás Gomes da, em *Futuro do setor dos pagamentos na União Europeia: análise das novas propostas regulatórias*, de 27-10-2023, disponível em <Futuro do setor dos pagamentos na União Europeia: análise das novas propostas regulatórias | Garrigues> (15-07-2024).

Romãnova, Inna; Grima, Simon; Spiter, Jonathan; Kudinska, Marina, "The Payment Services Directive II and Competitiveness: The Perspective of European Fintech Companies", *in European Research Studies Journal*, Volume XXI, Issue 2, 2018, pp. 3-22

Santos, Hugo Luz, "Plaidoyer por uma "distribuição dinâmica do ónus da prova" e pela "teoria das esferas de risco" à luz do recente acórdão do Supremo Tribunal de Justiça, de 18/12/2013: o (admirável) "mundo novo" no homebanking?"*, in Revista Electrónica de Direito*, Abril de 2014

Statista Research Department, *Open banking users worldwide in 2020 with forecasts to 2024, by region*, de 17-05-2023, disponível em < Open banking users worldwide by region | Statista> (26-05-2024)

Thasarathakumar, Lavan; Montgomery, Virginia, Evolution not revolution: European Commission publishes financial data access and payments package, de 30-06-2023, disponível em <Evolution not revolution: European Commission publishes financial data access and payments package - Hogan Lovells Engage> (18-07-2020)

Vasconcelos, Miguel Pestana, "A responsabilidade do banco por operações de pagamento não autorizadas no *online banking*, decorrente do novo regime de serviços de pagamento (RSP II)", *in Julgar*, n.º 42, 2020, pp. 191-208

Zago, Giovani, "Como a IoT está moldando os modelos de pagamento do futuro", de 31 janeiro de 2022, disponível em < Como a IoT está moldando os modelos de pagamento do futuro. (linkedin.com)> (09-06-2024).

JURISPRUDÊNCIA

Acórdão do Tribunal da Relação do Porto de 19-12-2023, (Paulo Duarte Teixeira)

Acórdão do Tribunal da Relação de Coimbra, de 10-12-2020, (Emídio Santos)

Acórdão do Tribunal da Relação de Lisboa, de 28-04-2022, (Luís Correia de Mendonça)

Acórdão do Tribunal da Relação do Porto, de 27-06-2022, (Mendes Coelho)

Acórdão da Relação de Évora, 12-04-2018, (Ana Margarida Lebre)

Acórdão da Relação de Lisboa de 15-03-2016, (Rijo Ferreira)

Acórdão da Relação de Coimbra de 15-01-2019, (Moreira do Carmo)

Acórdão da Relação do Porto, de 12-10-2023, (Ana Luísa Loureiro)

Acórdão do Tribunal da Relação de Lisboa, de 12-07-2018, (Higina Castelo)

Acórdão da Relação do Porto, de 13 de Junho de 2018 (Francisca Mota Vieira)

Acórdão da Relação de Lisboa, de 29-09-2022, (Maria de Deus Correia)

Acórdão do Tribunal da Relação do Porto, de 16-05-2023, (Rodrigues Pires)

Acórdão do Tribunal da Relação do Porto, de 08-03-2019, (Alexandra Pelayo)

Acórdão do Tribunal da Relação de Guimarães, de 07-06-2023, (José Alberto Martins Moreira Dias)

Acórdão do Supremo Tribunal de Justiça, de 23-01-2024, (Nelson Borges Carneiro)

Acórdão do Supremo Tribunal de Justiça, de 16-02-2023, (Catarina Serra)

Acórdão do Supremo Tribunal de Justiça, de 12-12-2023, (Manuel Capelo)

Acórdão do Supremo Tribunal de Justiça de 31-01-2019, (Helder Almeida)

Acórdão do Supremo Tribunal de Justiça, de 12-12-2023, (Manuel Capelo)

Acórdão do Supremo Tribunal de Justiça, de 18-12-2013, (Ana Paula Boularot)

TJUE, Ac.TJ, 2-set.-2021, Processo C-337/20, DM, LR c. Caise régionale de Crédit agricole mutuel (CRCAM)-Alpes-Provence, n.°34;

TJUE, Processo C-287/19, DenizBank AG, 11 de novembro de 2020, ECLI:EU:C:2020:897, § 75