DSP2: OPORTUNIDADES E DESAFIOS

TIAGO DA CUNHA PEREIRA

REVISTA DE DIREITO FINANCEIRO E DOS MERCADOS DE CAPITAIS, VOL. 1 (2019), NO. 5, 507-524

TIAGO DA CUNHA PEREIRA
Advogado-estagiário, Mestre em Direito e Gestão

DSP2: Oportunidades e Desafios

PSD2: Opportunities and Challenges

Resumo: O presente ensaio foca-se na análise do pacote legislativo encabeçado pela Segunda Diretiva de Serviços de Pagamento e das respetivas mudanças e novidades potenciadas pelo mesmo.

Palavras-chave: (i) DSP2; (ii) Serviços de Pagamento; (iii) Autenticação Forte do Cliente; (iv) Proteção dos Consumidores; (v) Serviços de Iniciação de Pagamentos.

Abstract: The present essay focuses on analysing the normative package spearheaded by the Second Payment Services Directive as well as the respective changes and novelties brought upon by it.

Keywords: (i) PSD2; (ii) Payment Services; (iii) Strong Customer Authentication; (iv) Consumer Protection; (v) Payment Initiation Services.

1. Enquadramento

Na sequência do acelerado desenvolvimento tecnológico a que temos assistido nos últimos anos e com vista à digitalização de um dos setores mais tradicionais no mercado único, a União Europeia levou a cabo uma revisão da Primeira Diretiva de Serviços de Pagamento ("DSP")[1]. O processo legislativo desencadeado deu origem a um pacote de disposições europeias[2] encabeçado pela Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno, a Segunda Diretiva de Serviços de Pagamento ("DSP2" ou "Diretiva"). Entre nós, a DSP2 foi transposta pelo do Decreto-Lei n.º 91/2018, de 12 de novembro, que aprova o regime jurídico dos serviços de pagamento e moeda eletrónica ("RJSPME").

A DSP2 visa primordialmente a abertura dos serviços de pagamento aos novos *players* no mercado; mercado esse que, até à redação da Diretiva, pertencia por excelência às instituições de crédito. Esta partilha de quota de mercado promove a eficiência dos vários agentes económicos, que agora se encontram mais próximos de um regime de concorrência perfeita. Um clima de concorrência entre prestadores de serviços de pagamento é ainda propício à alavancagem da inovação tecnológica, outra das bandeiras da DSP2. Pode roçar a ironia, aliás, pensar que a Diretiva visa promover avanços tecnológicos quando, por um lado, a necessidade de rever a DSP surge na sequência do aparecimento de novos intervenientes no mercado que, auxi-

[1] Referimo-nos à Diretiva 2007/64/CE do Parlamento Europeu e do Conselho, de 13 de novembro de 2007, relativa aos serviços de pagamento no mercado interno, entre nós transposta pela Lei n.º 84/2009, de 26 de agosto.

[2] Vejam-se, a título de exemplo o Regulamento Delegado (UE) 2017/2055 da Comissão, de 23 de junho de 2017, que completa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho no que diz respeito às normas técnicas de regulamentação para a cooperação e a troca de informações entre autoridades competentes relativamente ao exercício do direito de estabelecimento e da livre prestação de serviços das instituições de pagamento e o Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de novembro de 2017, que complementa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras.

liando-se das mais variadas *fintech*, se propuseram a comercializar serviços acrescentadores de valor junto de consumidores e empresas. Na verdade, a DSP2 vem reconhecer a existência e importância destes novos sujeitos, procurando liberalizar ao máximo a conjuntura legal europeia, por forma a garantir que futuros prestadores de novos serviços de pagamento não sintam os entraves sofridos pelos primeiros no acesso àquele que deve ser um mercado único cada vez mais digital. Neste sentido, estipula o considerando 21 da DSP2 que "*A definição de serviços de pagamento deverá ser tecnologicamente neutra e deverá permitir o desenvolvimento de novos tipos de serviços de pagamento, garantindo simultaneamente condições equivalentes para o exercício da atividade tanto aos prestadores de serviços de pagamento existentes como aos novos prestadores.*"

Se, por um lado, a abertura e a inovação são desejadas, é também certo que a multiplicação de prestadores de serviços de pagamento acarreta novos desafios para a proteção dos utilizadores, especialmente porque outrora o mercado se encontrava restrito a um ínfimo número de instituições de crédito, já sujeitas a inúmeros requisitos prudenciais[3]. De facto, a preocupação em proteger os utilizadores está patente em vários pontos da Diretiva, o que é apenas lógico se pensarmos que é sobre estes que impende o maior risco no ecossistema dos pagamentos – afinal, os serviços de pagamento não são mais do que meios para os utilizadores acederem e movimentarem os seus fundos. O aumento do número e tipo de prestadores de serviços de pagamento – nem todos incumbidos dos pesados deveres que impendem sobre as instituições de crédito – assim como da amplitude da definição destes serviços implica a adoção de medidas que assegurem, entre outros interesses, o combate à fraude e ao acesso indevido a contas de pagamento, a proteção dos dados pessoais dos utilizadores e a criação de regimes de responsabilidade proporcionais aos deveres próprios dos vários intervenientes nestes serviços.

[3] A este respeito, *vide* Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento, frequentemente apelidada de *Capital Requirements Directive IV* ("Diretiva dos Requisitos de Capital", em português) ou apenas "CRD IV".

Estamos, portanto, perante uma Diretiva ambiciosa que almeja abrir o mercado de serviços de pagamento a uma multiplicidade de intervenientes, fomentando assim a concorrência e a inovação tecnológica, enquanto assegura a proteção dos utilizadores. Prossigamos então para uma análise mais aprofundada sobre aquelas que consideramos serem as pedras-de-toque do pacote legislativo e regulamentar em torno da DSP2.

2. Novos serviços de pagamento

À semelhança do que sucedia na DSP, a definição de "serviço de pagamento" continua plasmada no artigo 4.º n.º 3[4], remetendo este, por sua vez, para o Anexo I à nova Diretiva. A diferença do Anexo I à DSP2 face ao Anexo à DSP reside no facto de esta primeira reconhecer expressamente o surgimento de dois novos serviços de pagamento: os serviços de iniciação de pagamentos e os serviços de informação sobre contas (n.os 7 e 8 do Anexo I, respetivamente). Também as definições destes dois novos serviços de pagamento podem ser encontradas no artigo 4.º da DSP2.

Nos termos da disposição supramencionada, um serviço de iniciação de pagamento é aquele segundo o qual se desencadeia uma ordem de pagamento a pedido de um utilizador do serviço de pagamento (doravante "USP"[5]) relativamente a uma conta de pagamento detida noutro prestador de serviços de pagamento[6]. Quer isto dizer que existe um prestador de serviços de pagamento que disponibiliza e gere a conta de pagamentos do utilizador (doravante "PSPGC"[7] [8]),

[4] Todas as referências a disposições normativas sem referência expressa a diploma legal devem ser entendidas como feitas à Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE.

[5] Ou "*Payment Service User – PSU*", em inglês).

[6] *Vide* artigo 4.º n.º 15.

[7] Em inglês, "*Account Servicing Payment Service Provider – ASPSP*"

[8] Figura prevista no n.º 17 do artigo 4.º da DSP2.

a quem o USP concede autorização para que um prestador de serviços de pagamento (doravante "PSP"[9]), *in casu*, um prestador de serviços de iniciação de pagamentos ("PSIP"[10]), aceda a certos dados financeiros da sua conta de pagamentos, por forma a iniciar uma ordem de pagamento a favor de um determinado beneficiário. Em termos práticos, talvez se afigure mais fácil explicar os fluxos de informação por passos:

i. O USP (ordenante da operação de pagamento) propõe-se a adquirir um bem ou serviço junto de um comerciante (beneficiário da operação de pagamento);
ii. O USP autoriza o PSIP a aceder à sua conta de pagamento;
iii. O comerciante envia ao PSIP os dados relevantes para que este possa executar a ordem de pagamento em nome do USP;
iv. O PSIP acede à conta de pagamentos do USP e atesta que existem fundos disponíveis para completar a operação de pagamento;
v. O PSIP fornece ao PSPGC do USP a informação sobre a conta do comerciante;
vi. O PSPGC do USP executa a ordem de pagamento e informa o PSIP;
vii. O PSIP recebe confirmação da execução e informa o comerciante;
viii. O comerciante disponibiliza o bem/serviço ao USP.

Já o serviço de informação sobre contas é descrito como um serviço em linha ("*online")* para a prestação de informações consolidadas sobre uma ou mais contas de pagamento detidas pelo mesmo USP junto de um ou mais PSPGC[11]. Definitivamente mais fácil de explanar, este serviço resume-se à agregação de contas de pagamento detidas pelo USP, por forma a que este tenha uma visão

[9] Curiosamente, a terminologia inglesa – *Payment Service Provider* – é também descrita pela sigla "PSP".
[10] Em inglês, "*Payment Initiation Service Provider – PISP*".
[11] *Vide* artigo 4.º n.º 16 e considerando 28.

global da sua situação financeira num dado momento. Esta agregação é feita por um prestador de serviços de informação sobre contas (doravante "PSIC"[12]), a quem o USP concedeu autorização para aceder a uma ou várias contas de pagamento, junto de um ou mais PSPGC.

O reconhecimento destes dois serviços de pagamento não é feito aleatória nem inocuamente. Se consultarmos o considerando 27, podemos ler que os serviços de iniciação de pagamentos "*(...) têm um papel a desempenhar nos pagamentos efetuados no âmbito do comércio eletrónico criando uma ponte telemática entre o sítio web do comerciante e a plataforma bancária em linha do prestador de serviços de pagamento que gere as contas do ordenante, a fim de iniciar pagamentos através da Internet com base numa transferência a crédito*". Existe, portanto, um interesse na regulação dos serviços iniciação de pagamento, uma vez que constituem uma importante ferramenta para a promoção do mercado único interno[13] num tempo em que este é (e se quer) cada vez mais digital.

A preocupação primária em legislar sobre os serviços de informação sobre contas pende mais sobre a proteção dos utilizadores do que propriamente sobre o interesse económico. A DSP2 reconhece que estes serviços apenas podem existir mediante atribuição de proteção adequada dos dados relativos à(s) conta(s) do USP, bem como de certeza jurídica quanto ao estatuto de PSIC[14].

Visto, pois, que os novos serviços de pagamento suscitam interesse, cumpre agora estudar como é que a DSP2 se propõe a prevenir e mitigar as preocupações simultaneamente manifestadas.

[12] Em inglês, "*Account Information Service Provider – AISP*".

[13] Para este objetivo contribuiu igualmente o Regulamento (UE) n.º 260/2012 do Parlamento Europeu e do Conselho, de 14 de março de 2012, que estabelece requisitos técnicos e de negócio para as transferências a crédito e os débitos diretos em euros e que altera o Regulamento (CE) n. o 924/2009 ("Regulamento SEPA"), ao estabelecer a regra segundo a qual, em princípio, os encargos cobrados por um PSP não podem ser discriminatórios em função da nacionalidade do ordenante ou do beneficiário.

[14] *Vide* considerando 28 e artigo 67.º. Voltaremos a esta temática aquando da nossa análise sobre a proteção dos utilizadores ao abrigo da DSP2.

3. Proteção dos utilizadores

O regime protecionista conferido aos USPs é uma matéria bastante fragmentada ao longo do pacote legislativo e regulamentar em torno da DSP2. Como tal, e por forma a obtermos uma visão completa, consideramos oportuno dividir o estudo desta temática por tópicos, analisando cada um destes à luz das respetivas normas legais e regulamentares existentes à data.

3.1. Registo de prestadores de serviços de pagamento

A DSP, no seu artigo 13.º, sujeitava o exercício da atividade de instituição de pagamento a registo junto dos Estados-Membros em que a instituição operasse. Tal registo devia inclusive referir quais os serviços de pagamento que esta se encontrava autorizada a levar a cabo. Ainda assim, com a evolução do comércio eletrónico, a DSP2 entendeu necessário assegurar uma camada adicional de proteção entre fronteiras. Como tal, instituiu que a Autoridade Bancária Europeia ("EBA") deve criar um registo eletrónico central de todas as instituições de pagamento, cabendo aos Estados-Membros garantir que este se mantém atualizado[15].

As normas técnicas de regulamentação que definem os requisitos para o desenvolvimento, gestão e manutenção do supracitado registo eletrónico central, assim como o acesso à informação nele disponível, são delineadas no Regulamento Delegado (UE) 2019/411 da Comissão, de 29 de novembro de 2018. Como se compreenderá, a implantação de um registo centralizado europeu de instituições de pagamento implica esforços de cooperação entre os vários supervisores nacionais e a EBA. Foi com este desafio em mente que, na mesma data, a Comissão adotou o Regulamento de Execução (UE) 2019/410, estabelecendo normas técnicas que regulam a estrutura e os pormenores da informação a notificar pelos vários Estados-Membros à EBA. Desta forma, a Comissão procurou uniformizar o

[15] *Vide* considerando 42 e artigo 15.º da DSP2.

processo de reporte, com vista à uniformização da informação constante da base de dados europeia[16].

Por fim, note-se que o registo centralizado não preclude a continuidade do registo nacional imposto pela DSP, agora plasmado no artigo 14.º da DSP2.

3.2. Autenticação forte do cliente

Com o crescimento do comércio eletrónico, acentuaram-se também as preocupações com a fraude que o anonimato da internet tanto propicia. Servindo-se de referências diretas aos riscos provenientes de cartões com a tecnologia *contactless* e à mistificação de interfaces (vulgo "*phishing*"), a DSP2 defende o princípio da proporcionalidade entre o risco inerente a um determinado serviço de pagamento e as medidas de segurança que devem restringir o mesmo[17].

A autenticação forte do cliente ("AFC")[18] surge como a medida de segurança entendida necessária em três cenários concretamente definidos no número 1 do artigo 97.º da DSP2: (i) o acesso *online* a uma conta de pagamento; (ii) a iniciação de uma operação de pagamento eletrónico e (iii) a realização de uma ação, através de um canal remoto, que possa envolver um risco de fraude no pagamento ou outros abusos. Este último preceito, na nossa opinião, foi intencionalmente redigido de uma forma vaga, de modo a acautelar novos cenários de risco que venham a fruir dos avanços tecnológicos em sede de pagamentos.

Este método de autenticação consiste na utilização de um mínimo de dois elementos pertencentes às categorias "conhecimento" (algo que só o utilizador conhece[19]), "posse" (algo que só o utilizador pos-

[16] O registo central europeu pode ser encontrado no sítio da EBA em: https://euclid.eba.europa.eu/register/pir/disclaimer

[17] *Vide* considerando 96 da DSP2.

[18] Em inglês, "*Strong Customer Authentication – SCA*"

[19] Por exemplo, a cor favorita do utilizador.

sui[20]) e inerência (algo que só o utilizador é[21]), de forma independente – ou seja, se a fiabilidade de um destes elementos for comprometida, a dos restantes manter-se-á imaculada[22].

Com vista ao reforço da segurança dos USP, a autenticação forte deve ser efetuada de forma dinâmica, para que cada operação, com um montante e beneficiário específicos, usufrua de um processo de autenticação próprio. O mesmo será dizer que a autenticação previamente efetuada não dispensa o USP de um novo procedimento, sempre que este se encontre perante um dos três cenários em que o mesmo é devido. Existem, no entanto, exceções. Por exemplo, a autenticação forte para o acesso online a uma conta de pagamentos isenta o USP deste requisito para o acesso em linha à referida conta de pagamentos por um período de 90 dias[23]).

Reconhecendo a especial complexidade técnica deste procedimento, a DSP2 encarregou a EBA de elaborar normas técnicas de regulamentação sobre a AFC[24]. Esta obrigação materializou-se no Regulamento Delegado 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. Foi precisamente este diploma que entrou em vigor no passado dia 14 de setembro, resultando numa onda de divulgação sobre as novas regras dos serviços de pagamento, tanto pelas instituições de crédito como pelos meios de comunicação tradicionais.

[20] Por exemplo, o número de telemóvel do utilizador.

[21] Por exemplo, os dados biométricos do utilizador – máxime, a sua impressão digital.

[22] *Vide* número 30 do artigo 4.º da DSP2.

[23] *Vide* artigo 10.º, número 2 alínea b) do Regulamento Delegado 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.

[24] *Vide* considerando 107 e artigo 98.º da DSP2.

3.3. Proteção de dados pessoais

A DSP2, no seu considerando 89, reconhece que a prestação de serviços de pagamento pode implicar o tratamento de dados pessoais. Este mesmo considerando faz referência à Diretiva 95/46/CE do Parlamento Europeu e do Conselho e ao Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, ambos para efeitos de tratamento de dados pessoais no âmbito dos serviços de pagamento. Tais referências encontram-se desatualizadas, uma vez que a Diretiva 95/46/CE foi revogada pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 ("Regulamento Geral de Proteção de Dados" – "RGPD") e o Regulamento (CE) n.º 45/2001 foi adaptado por forma respeitar os princípios por este instituídos[25]. No entanto, a remissão justifica-se pelo facto de o processo legislativo que culminou na adoção da DSP2 ter tido início em 2013, previamente à adoção do RGPD. Assim sendo, e com recurso a uma interpretação atualista, entendemos que em matéria de serviços de pagamento se devem aplicar os princípios e regras constantes do RGPD. Tal convicção é reforçada pelo já referido considerando 89 da DSP2, quando nos diz que o tratamento de dados ao abrigo da Diretiva deve ter um objetivo exato, uma base jurídica aplicável, requisitos de segurança, respeito pelos princípios da necessidade, da proporcionalidade, da limitação da finalidade e do período de conservação dos dados – todos concretizados pelo RGPD. É ainda feita uma referência à proteção de dados desde a conceção, uma das bandeiras encontradas no artigo 25.º do Regulamento.

Consultando o artigo 94.º da DSP2, entendemos que o enfoque da proteção de dados pessoais no âmbito da Diretiva visa prevenir, investigar e detetar fraudes em matéria de pagamentos. O tratamento destes dados por parte dos PSP encontra-se ainda restringido pelo princípio da necessidade e o seu tratamento e conservação dependem do consentimento expresso do USP. Entendemos que a referência ao princípio da proporcionalidade não era necessária, uma vez que, como já vimos, o mesmo já consta do regime geral

[25] *Vide* considerando 17 e artigo 94.º do RGPD.

europeu em matéria de proteção de dados pessoais. Sujeitar o tratamento dos dados do utilizador ao seu expresso consentimento também nos parece desnecessário, uma vez que tal tratamento é requisito para a execução do contrato entre o USP e PSP, pelo que dispensa a prestação de consentimento nos termos do artigo 6.º n.º 1 alínea b) do RGPD[26]. Por fim, discordamos ainda que a conservação dos dados tratados careça do consentimento expresso USP, uma vez que o PSP necessita de conservar estes dados pelo período necessário para provar, nos termos do artigo 72.º n.º 1 da DSP2, que determinada operação foi autenticada, devidamente registada e contabilizada, e que não foi afetada por qualquer avaria técnica ou por outra deficiência do serviço por este prestado. Ou seja, configura uma situação de tratamento de dados pessoais para cumprimento de uma obrigação legal a que o responsável pelo tratamento – o PSP – está sujeito, dispensando por isso o consentimento do titular dos dados – o USP – nos termos do artigo 6.º n.º 1 alínea c) do RGPD.

Não obstante a nossa discordância com o modo como a proteção de dados pessoais foi codificada na Diretiva, existe a intenção em proteger os USP contra fraudes que derivem do uso indevido dos seus dados pessoais, mormente para o acesso às respetivas contas de pagamento. Esta preocupação justifica-se especialmente na DSP2 pelo facto de a AFC ser realizada, em parte, através do recurso a dados pessoais. Assim, facilmente se entende que uma desproteção do consumidor neste domínio poderá facilmente comprometer o sistema europeu de pagamentos eletrónicos que tanto se pretende implementar.

Ainda relacionada com este tópico está a publicação, por parte da EBA, de recomendações técnicas sobre a subcontratação a prestadores de serviços em nuvem (vulgo "*cloud*")[27]. Entre nós, o Banco de Portugal fez saber que se compromete a cumprir com o

[26] Existe ainda o problema da aferição do consentimento nestas situações. Neste sentido, *vide* Tiago Correia Moreira/Inês Antas de Barros/Isabel Ornelas, *Partilha de dados pessoais e operação bancária aberta* em Fintech: Novos Estudos Sobre Tecnologia Financeira, coord. António Menezes Cordeiro/Ana Perestrelo de Oliveira/Diogo Pereira Duarte, Almedina (2019), 149-156.

[27] *Vide* EBA/REC/2017/03.

disposto nas referidas recomendações através da Carta Circular n.º CC/2019/00000025.

3.4. Responsabilidade do utilizador e do prestador de serviços de pagamento

A DSP, no seu artigo 56.º, impunha a obrigação de o USP comunicar ao respetivo PSP a perda, roubo, apropriação abusiva ou qualquer outra apropriação indevida do seu instrumento de pagamento. Regra geral, após esta comunicação, a DSP limitava a responsabilidade do USP por operações de pagamento não autorizadas com o seu instrumento de pagamento a 150 euros[28]. A DSP2, no seu artigo 74.º veio a reduzir este limite para 50 euros[29]. O legislador europeu entendeu que esta redução incentiva o USP a notificar o respetivo prestador do acontecimento sem demora indevida, mitigando assim o risco de operações não autorizadas[30]. Estes limites de responsabilidade conhecem as exceções já firmadas pela DSP, como os casos de atuação fraudulenta ou negligência grosseira por parte do USP, agora previstos ao longo do artigo 74.º da DSP2. Não obstante, é inegável que nos encontramos perante mais uma novidade que concorre para a proteção dos utilizadores.

Por outro lado, na esfera dos PSPGC e dos PSIP surge agora a possibilidade de responsabilização por não execução, falhas na execução ou execução tardia de operações de pagamento. Os artigos 89.º e 90.º, respetivamente, estabelecem a data-valor para o reembolso ou correta execução das operações de pagamento nos casos *supra* elencados, consoante o USP seja, respetivamente, ordenante ou beneficiário da operação viciada. Independentemente da existência de responsabilidade ao abrigo destes preceitos, o USP tem a faculdade de solicitar ao PSP que envide imediatamente esforços para rastrear determinada operação de pagamento e lhe comunique os

[28] *Vide* artigo 61.º da DSP.

[29] Na DSP2, a obrigação de comunicação encontra-se plasmada no artigo 69.º. Nota ainda para a precisão do legislador europeu na substituição do termo "roubo" por "furto".

[30] *Vide* considerando 71 e artigo 74.º da DSP2.

resultados obtidos, sem que o utilizador incorra em qualquer custo. Ademais, os PSP respondem ainda perante os USP por quaisquer encargos e juros a que estes últimos estejam sujeitos em consequência da não execução, execução incorreta ou execução tardia de uma operação de pagamento.

Em abono do espírito de liberalização do mercado de serviços de pagamento, o legislador europeu entendeu que seria desproporcional sujeitar PSIP e PSIC a requisitos de capitais próprios (à semelhança dos PSP tradicionais – as instituições de crédito), uma vez que, se estes exercerem exclusivamente as atividades de iniciação de pagamentos e informação sobre contas, não detêm fundos dos clientes. Como tal, entendeu que estes sujeitos apenas devem subscrever um seguro de responsabilidade civil profissional ou garantia equivalente, delegando na EBA a fixação de critérios para determinação do montante mínimo a segurar[31]. Entre nós, os critérios de fixação do capital mínimo e os demais requisitos mínimos do seguro de responsabilidade civil profissional dos PSP que exerçam exclusivamente os serviços de iniciação de pagamentos e/ou de informação sobre contas constam da Portaria n.º 238/2019, de 30 de julho. Também esta é uma novidade que inegavelmente concorre para a proteção dos USP.

Aspeto diverso que contribui para a proteção dos utilizadores, ainda que indiretamente, é o agravamento do regime contraordenacional. Ambas as Diretivas, como aliás já é prática, delegam nos Estados-Membros a codificação de sanções efetivas proporcionais e dissuasivas. No entanto, o Decreto-Lei n.º 91/2018, de 12 de novembro é dotado de um leque de infrações mais extensivo face ao Decreto-Lei n.º 317/2009, de 30 de outubro, que transpôs a DSP para o ordenamento jurídico português, por forma a acautelar as novas obrigações impostas pela DSP2[32]. Talvez pela importância cres-

[31] *Vide* considerando 35 e número 4 do artigo 5.º da DSP2, assim como as *EBA/GL/2017/08 – Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarntee under Article 5(4) of Directive (EU) 2015/2366 (PSD2)*, de 7 de julho de 2017.

[32] Cfr. artigo 150.º do Decreto-Lei n.º 91/2018, de 12 de novembro com o artigo 94.º do Decreto-Lei 317/2009, de 30 de outubro.

cente dos serviços de pagamento, o legislador pátrio tomou ainda a decisão de agravar o teto máximo da coima aplicável a pessoas singulares aquando da prática de infrações especialmente graves para o montante de 5.000.000€ (cinco milhões de euros), curiosamente equiparando-o à coima máxima a que as pessoas coletivas se encontram sujeitas[33].

Por tudo quanto exposto, resulta claro, na nossa opinião, que a proteção dos USP é a maior das preocupações vertidas ao longo do texto da DSP2 e do respetivo Decreto-Lei que a transpõe.

4. Oportunidades

As possibilidades apresentadas pela nova Diretiva são várias e estendem-se ao longo de vários setores. A prestação de serviços de pagamento, outrora circunscrita a um número reduzido de *players*, é hoje um nicho à mercê da crescente onda de *fintech* que tem marcado o ritmo da marcha em direção a uma economia digital. Com a abertura deste segmento de mercado, sociedades não financeiras veem agora a possibilidade de alargar o respetivo leque de serviços, através de soluções pouco onerosas (tanto para comerciantes como para consumidores) ao mesmo tempo que apresentam aos clientes uma experiência mais simples e integrada. Tal será o caso, por exemplo, de um grande retalhista que se constitua como PSIP. Os serviços de iniciação de pagamentos permitem ainda efetuar compras *online* sem recurso a cartões de pagamento, aumentando assim o número de consumidores no comércio eletrónico[34].

Por outro lado, liberalização do mercado de serviços de pagamento fomenta o desenvolvimento tecnológico, incentivando as *fintech* a desenvolverem novos serviços de pagamento.

[33] Previamente, este montante era de 5.000.000€ (cinco milhões de euros) para as pessoas coletivas e 2.000.000€ (dois milhões de euros) para as pessoas singulares. Cfr. artigo 151.º do Decreto-Lei n.º 91/2018, de 12 de novembro com o artigo 95.º do Decreto-Lei n.º 317/2009 de 30 de outubro.

[34] *Vide* considerando 29 da DSP2.

A crescente e justificada preocupação com a segurança nas operações de pagamento constitui uma oportunidade para aqueles que prestem serviços de autenticação e de segurança da informação. Prevemos que, num futuro próximo, estas entidades andem de mão dada com os PSP, quer para assegurar a segurança dos serviços prestados por estes últimos, quer para os ajudar na conceção de novos serviços de pagamento.

O próprio ato legislativo de sujeitar os PSP que prestem exclusivamente serviços de informação sobre contas e/ou serviços de iniciação de pagamentos à subscrição de um seguro de responsabilidade civil profissional constitui uma oportunidade para o setor segurador. Por sua vez, também a procura dos seguros de ataques informáticos (ou "ciber ataques") sai reforçada pelo paradigma imposto pela DSP2.

No entanto, o maior sintoma da nova Diretiva reside no já referido Regulamento Delegado 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. Segundo o plasmado na Secção 2 deste diploma, os PSPGC (leia-se "bancos") que ofereçam contas de pagamentos *online* devem dispor de, pelo menos, uma interface que permita (i) aos prestadores de serviços de informação sobre contas, prestadores de serviços de iniciação de pagamentos e prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartão identificarem-se junto do PSPGC, (ii) aos prestadores de serviços de informação sobre contas comunicar de forma segura para pedir e receber informações sobre uma ou mais contas de pagamento designadas e as respetivas operações de pagamento associadas, e (iii) aos prestadores de serviços de iniciação de pagamentos comunicar de forma segura para iniciar uma ordem de pagamento a partir da conta de pagamento do ordenante e receber todas as informações sobre a iniciação da operação de pagamento e todas as informações acessíveis aos PSPGC sobre a execução da operação de pagamento[35].

[35] *Vide* artigo 30.º do referido Regulamento Delegado.

São duas as opções que o artigo 31.º do Regulamento Delegado confere aos PSPGC: criar uma interface dedicada para cumprimento das condições suprarreferidas, ou, em alternativa, permitir que os PSP mencionados utilizem as (já existentes) interfaces destinadas à autenticação e comunicação entre USP e PSPGC. Em termos simples, os bancos veem-se forçados a criar uma interface própria nos termos acima referidos ou a conceder aos PSP acesso às interfaces que utilizam para autenticação e comunicação com os seus clientes. Quer as interfaces dedicadas quer as interfaces que o PSPGC utiliza devem obedecer a normas de comunicação emitidas por organizações de normalização internacionais ou europeias, por forma garantir a interoperabilidade técnica entre o PSPGC e os vários PSP que pretendam aceder a contas de pagamento detidas por USP junto desse mesmo PSPGC[36]. No fundo, os PSP não precisam de se ocupar do pesado e dispendioso trabalho técnico de desenvolver interfaces compatíveis com as dos vários PSPGC existentes à data, uma vez que estes foram incumbidos de criar uma interface dedicada harmonizada ou de harmonizar e disponibilizar as suas interfaces internas. Os ganhos são inegáveis para os PSP, que apenas se limitarão a usufruir de uma estrutura completamente edificada e suportada pelos PSPGC.

5. Desafios

Na sombra das várias oportunidades expostas pela DSP2, encontram-se constrangimentos e inquietações que se propõem a ameaçar a sua integral efetivação. A preocupação mais notória é certamente a que advém da abertura do mercado a novos intervenientes. Ao passo que outrora os serviços de pagamento estavam restritos a uma oligarquia, no pós-DSP2 assistimos a uma multiplicação dos pontos de acesso à informação pessoal e financeira dos USP – muitos dos quais despidos de sistemas informáticos tão robustos como os dos incumbentes tradicionais. O crescimento numérico de PSP

[36] *Vide* artigo 30.º n.º 3 do Regulamento Delegado.

constitui uma oportunidade para todos aqueles que pretendem aceder indevidamente aos dados dos utilizadores e um teste para as medidas de segurança adotadas na sequência da Diretiva.

Preocupação diversa é a da falta de concretização do artigo 36.º, norma que estatui, a nosso ver vagamente, as condições de acesso por parte das instituições de pagamento às contas de pagamento dos utilizadores. Plasma esta norma que o acesso deve ser concedido *numa base objetiva, não discriminatória e proporcionada* e de modo suficientemente alargado, por forma a permitir a prestação eficiente e sem entraves dos vários serviços de pagamento. *In fine*, refere ainda que a instituição de pagamento (leia-se "o PSPGC") pode apresentar à autoridade competente os motivos devidamente fundamentados de uma eventual de recusa de acesso. Ora, a falta de detalhe, tanto nos critérios de concessão como nos fundamentos de recusa, culminará provavelmente na fixação de critérios dispares ao longo dos vários Estados-Membros o que, ironicamente, se afigura um entrave à conceção de um mercado único. Cremos que este é mais um objetivo cuja concretização deveria impreterivelmente ter passado pela EBA.

6. Conclusões

A DSP2 assume um papel disruptivo no mercado de serviços de pagamento. Acreditamos que a Diretiva reúne as condições necessárias para concretizar a tão desejada liberalização dos serviços de pagamento sem comprometer a segurança dos utilizadores. Não obstante, cremos que a falta de concretização de algumas das suas normas poderá resultar em transposições e interpretações nacionais diferenciadas, possivelmente criando barreiras legais e regulatórias à europeização da atividade dos novos prestadores de serviços de pagamento. Em última instância, caberá ao Tribunal de Justiça da União Europeia levar a cabo a harmonização dos critérios de que o legislador europeu não se ocupou.

Bibliografia

Tiago Correia Moreira/Inês Antas de Barros/Isabel Ornelas, *Partilha de dados pessoais e operação bancária aberta* em Fintech: Novos Estudos Sobre Tecnologia Financeira, coord. António Menezes Cordeiro/Ana Perestrelo de Oliveira/Diogo Pereira Duarte, Almedina (2019), 149-156.