

Publicação disponível em: <https://blook.pt/publications/publication/179ecbbf9e20/>

DSP2 E RGPD: UMA DICOTOMIA NAS SUAS PARECENÇAS. UMA VISÃO PORTUGUESA SOBRE O ASSUNTO

FRANCISCO CHILÃO ROCHA

REVISTA DE DIREITO FINANCEIRO E DOS MERCADOS DE CAPITALIS, VOL. 2 (2020), NO. 9, 355-367



FRANCISCO CHILÃO ROCHA
Advogado-Estagiário da PLMJ

DSP2 e RGPD: Uma dicotomia nas suas parecências. Uma visão portuguesa sobre o assunto

*PSD2 and GDPR: A dichotomy in its likeliness.
A Portuguese view on the matter*

RESUMO: Nos últimos anos entraram em vigor dois diplomas da União Europeia, o RGPD e a DSP2, que apresentam uma inovação há muito pretendida. É, principalmente, um ansiado passo regulatório a fim de colocar as FinTechs em pé de igualdade com os prestadores de serviços de pagamento tradicionais, devolvendo a proteção de dados. Contudo, cumpre melhor definir e concretizar alguns dos aspetos, a nosso ver, mais relevantes dos dois diplomas em questão. Compara-se, assim, como os dois diplomas abordam os tópicos do consentimento, dever de informação e dos dados pessoais.

Palavras-chave: (i) RGPD; (ii) DSP2; (iii) Consentimento; (iv) Dever de informação; (v) Dados Pessoais

ABSTRACT: *In recent years two European Union acts entered into force, the GDPR and the PSD2, presenting a long-awaited innovation. It is, above all, an eagerly awaited regulatory step to put FinTechs on an equal footing with traditional payment service providers, giving data more protection. However, some of the most relevant aspects of the two pieces of legislation in our view need to be better defined and developed. It is, thus, compared how both diplomas approach the topics of consent, information obligation and personal data.*

Keywords: (i) *GDPR*; (ii) *PSD2*; (iii) *Consent*; (iv) *Information Obligation*; (v) *Personal Data*.

1. Enquadramento

A União Europeia tem vindo a dar passos importantes no que toca à modernização dos mais variados setores que a compõem¹, tendo em 2016 e 2018 entrado em vigor os dois diplomas em destaque neste artigo. Falamos do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016 (doravante “RGPD”), que entrou em vigor a 25 de maio de 2018, e a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro (doravante “DSP2”), que entrou em vigor a 12 de janeiro de 2016.

Comprometemo-nos, deste modo, a estabelecer uma análise comparativa nos aspetos que nos parecem merecer destaque ao abrigo dos dois principais diplomas em discussão, retratando o seu contexto e aplicação em Portugal. Neste caso, falamos do consentimento, dever de informação e proteção de dados, comparando as principais diferenças e semelhanças entre os dois diplomas comunitários.

1.1. RGPD

Em janeiro de 2012, a Comissão Europeia apresentou a primeira proposta de regulamento sobre a proteção de dados pessoais, com o objetivo inicial de proteger os cidadãos face ao risco emergente das soluções tecnológicas que existiam, pensando também nas futuras.

Não obstante tratar-se de um Regulamento europeu², o RGPD refere nos seus considerandos³ que, apesar de ser conveniente asse-

¹ Tal decorre da reunião do Conselho Europeu ocorrida em Lisboa, nos dias 23 e 24 de março de 2000, com vista à criação de um objetivo comum para a União de forma a fortalecer a empregabilidade, uma reforma económica e maior coesão social. Disponível em https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/00100-r1.en0.htm.

² Gozando, conforme o artigo 288.º do Tratado sobre o Funcionamento da União Europeia, de aplicabilidade direta, dado o seu carácter geral e obrigatoriedade.

³ Cfr. considerando 10 RGPD.

gurar-se a aplicação coerente e homogénea das regras no que diz respeito ao tratamento de dados pessoais, é permitido aos Estados-Membros aprovar ou manter disposições nacionais para especificar a aplicação destas regras. Mais, é assegurada alguma margem de manobra para esta inclusão nacional, inclusive no tocante aos “dados sensíveis”⁴. Pelo que, embora bem-vinda, não se entende a adoção especialmente tardia⁵, da Lei n.º 58/2019, de 8 de agosto⁶.

1.2. DSP2

No seguimento da primeira Diretiva de Serviços de Pagamento, de 2007, surge a DSP2. Dada a evolução do *ecommerce* na União, assim como o incremento de pagamentos via telefónica, urgia uma maior prevenção de fraude e maior segurança para o consumidor.

Por sua vez, a DSP2, enquanto Diretiva, apenas vincula o Estado-Membro quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios⁷. Dada a transposição obrigatória no prazo de dois anos, entrou em vigor a 13 de novembro de 2018 o Decreto-Lei n.º 91/2018, de 12 de novembro, que estabelece o novo Regime Jurídico dos Serviços de Pagamento e de Moeda Eletrónica (“RJSPME”).

⁴ Embora o diploma inicie o desenvolvimento sobre o assunto, conforme o considerando 51 RGD.

⁵ Como referido em comunicado da Comissão Europeia de 24 de julho de 2019, Portugal foi um dos 3 últimos países europeus a atualizar a sua legislação nacional, de forma a estar conforme o RGD. Disponível em https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4449.

⁶ Para mais detalhe referente à aplicação em Portugal e os desafios inerentes, remetemos para o Parecer n.º 20/2018, da Comissão Nacional de Proteção de Dados. Disponível em: <http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a5763765130394e4c7a464451554e45544563765247396a6457316c626e527663306c7561574e7059585270646d46446232317063334e686279396a5a57593359544d794f4330325a44526c4c54526c4e546b74596a41304e4331694e54426d4f5449314d6a64684d7a45756347526d&fich=cef7a328-6d4e-4e59-b044-b50f92527a31.pdf&Inline=true>

⁷ Cfr. artigo 288.º, 3.º parágrafo do Tratado sobre o Funcionamento da União Europeia.

Embora a DSP2 procure a inovação do mercado, através da introdução de proteções e melhores definições de forma a auxiliar a entrada de *FinTechs*⁸ enquanto Prestadores de Serviços de Pagamento (PSP)⁹ ou mesmo enquanto Instituições de pagamento autorizadas¹⁰, como as alternativas digitais existentes, o receio da possibilidade de aplicação de coimas leva a que a maioria dos incumbentes (as instituições financeiras tradicionais), não arrisquem na inovação.

2. Aspetos relevantes

2.1. Consentimento

Um pilar do RGPD, já consolidado pelo TJUE¹¹, prende-se com o consentimento¹². Assim como o é na DSP2, ao ser exigido que “uma operação de pagamento só seja considerada autorizada se o ordenante tiver dado o seu consentimento”¹³. De notar que as referências ao consentimento são frequentes na Diretiva.

O RGPD assenta o seu entendimento no facto de o consumidor/ utilizador ter de dar o seu consentimento ao tratamento de dados e que este tem de ser dado de forma livre, específica, informada, inequívoca e clara¹⁴. Como se retira da *Guideline* 05/20 da *European*

⁸ Deparámo-nos com várias definições para a noção de Fintechs. Seguindo a noção simplificada de SCHUEFFEL no seu artigo de 2016 “Taming the Beast: A Scientific Definition of Fintech”, “Fintech é uma nova indústria financeira que aplica tecnologia para melhorar atividades financeiras”. A própria palavra Fintech deriva da combinação das palavras *Financial* (Financeiro) e *Technology* (Tecnologia).

⁹ Cfr. artigo 4.º, ponto 11 DSP2.

¹⁰ Cfr. artigo 4.º, ponto 4 DSP2.

¹¹ Cfr. Acórdão C-673/17 “*Planet49*”, de 1 de outubro de 2019. De notar que pese embora o Acórdão se reportar ao tema de *cookies*, regulado pela diretiva *ePrivacy*, a legislação geral continua a ser o RGPD.

¹² Cfr. artigo 4.º, ponto 11 e artigo 6.º, n.º 1, alínea a RGPD.

¹³ Cfr. artigo 64.º, alínea 1 DSP2.

¹⁴ Cfr. artigo 11.º, n.º 11 RGPD. Ademais, o consentimento é um dos fundamentos legais em que o tratamento de dados pessoais tem de se basear, nos termos do artigo 6.º do mesmo Regulamento.

Data Protection Board (EDPB)¹⁵, adotada a 4 de maio de 2020, o consentimento só pode ser uma base legal apropriada se for oferecido ao titular dos dados um controlo e uma escolha genuína no que respeita à aceitação ou recusa das condições oferecidas ou à sua recusa sem prejuízo.

No entanto, não é possível encontrar o mesmo entendimento na DSP2. O máximo que a DSP2 identifica é a necessidade de um consentimento “expresso”¹⁶. Não obstante, o consentimento expresso ao abrigo da DSP2 é diferente do consentimento (expresso) ao abrigo do RGPD. O consentimento expresso ao abrigo do Artigo 94, n.º 2 da DSP2 é, no entender do EDPB¹⁷, mormente um requisito adicional de natureza contratual.

Ademais, o RGPD, como já havia sido referido, oferece uma visão mais conservadora. Um exemplo disso é o facto de o consentimento não poder expirar automaticamente, devendo ser o titular dos dados a retirar o mesmo, podendo fazê-lo a qualquer momento¹⁸. Já a DSP2 dispõe de uma noção menos restrita, definindo uma janela temporal a partir do qual o consentimento não poderá ser retirado¹⁹, através do carácter irrevogável de uma ordem de pagamento²⁰.

Outro ponto em conflito entre os dois diplomas prende-se com o facto de, no RGPD, a informação relativa à possibilidade de retirar o consentimento dever ser informada ao titular de dados²¹. Esta informação é omissa na DSP2.

Ademais, ao longo da DSP2 há uma omissão da necessidade de incumbentes obterem dos seus clientes o consentimento para partilhar o acesso aos seus dados a Prestadores de Serviços de Informação sobre Contas e Prestadores do Serviço de Iniciação de Pagamento,

¹⁵ Disponível, apenas em inglês, em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt

¹⁶ Cfr. artigo 65.º, 66.º, 67.º e 94.º DSP2.

¹⁷ Cfr. ponto 3 da Guideline 06/20, adotada a 17 de julho de 2020, relativa à interligação entre a DSP2 e RGPD. Disponível, apenas em inglês, em: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202006_interplaypsd2andgdpr.pdf

¹⁸ Cfr. artigo 7.º, alínea 3 RGPD.

¹⁹ Cfr. artigo 64.º, alínea 3 DSP2.

²⁰ Cfr. artigo 80.º DSP2.

²¹ Cfr. artigo 7.º, alínea 3 RGPD.

através das *interfaces* dos incumbentes, como as *homebanking apps* – o chamado *silent party data*²².

Esta questão encontra o seu paralelo com a questão do direito à portabilidade dos dados²³ no RGD, considerando, no entanto, a difícil questão de saber que parte deverá obter o consentimento.

Seguindo o alinhamento do RGD, a portabilidade requer que os responsáveis pelo tratamento sejam, pelo menos, encorajados a desenvolver as devidas medidas técnicas de forma a salvaguardar que atuam no legítimo interesse dos titulares²⁴. Como é referido no próprio Regulamento, o titular dos dados deverá recebê-los “num formato estruturado, de uso corrente e de leitura automática”²⁵. Além disso, a portabilidade dos dados não impõe ao responsável pelo tratamento a obrigação de conservar os dados pessoais durante um prazo superior ao necessário ou que exceda qualquer período de conservação especificado²⁶. Já a DSP2 confirma esta linha de raciocínio, assegurando que, por exemplo, o PSIC apenas tenha acesso a informação por um propósito específico, solicitado pelo utilizador²⁷.

Desta forma, parece-nos que será necessária uma dupla confirmação de consentimento, onde cada interveniente atua enquanto responsável pelo tratamento dos dados pessoais que lhe diz respeito.

²² Remetendo-nos ao exemplo presente em carta endereçada pelo Comité Europeu para a Proteção de Dados à Eurodeputada Sophie in't Veld a 5 de julho de 2018, referindo que tal ocorre, por exemplo, quando o USP A dá o seu consentimento expresso a um PSIP para tratar os seus dados, de forma a enviar dinheiro ao USP B. Não havendo relação contratual entre este USP B e o PSIP, questiona-se se este último poderá tratar dados pessoais de B, de forma a prosseguir com o pagamento – agindo enquanto *silent party*. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/news/psd2_letter_en.pdf.

²³ Este direito, elencado nos considerandos 68, 73 e 156 e no artigo 20.º RGD, permite ao titular dos dados receber os mesmos que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, “num formato estruturado, de uso corrente e de leitura automática”, sendo permitido que os transmita a outro responsável pelo tratamento sem que o primeiro responsável possa impedir.

²⁴ Cfr. considerando 68 RGD.

²⁵ Cfr. artigo 20.º, n.º 1 RGD.

²⁶ Cfr. pág. 7 das Orientações sobre o direito à portabilidade dos dados, do Grupo do Artigo 29.º para a Proteção de Dados, adotadas a 13 de dezembro de 2016. Disponível em: https://www.cnpd.pt/home/rgpd/docs/wp242rev01_pt.pdf

²⁷ Cfr. artigo 67.º, n.º 2, alíneas a, d e f DSP2.

Por último, de ressaltar que a DSP2 prevê que o procedimento de comunicação do consentimento é acordado entre o ordenante e o prestador de serviços²⁸, que significará que os conflitos entre RGD e DSP2 deixam de existir quando o interesse legítimo é fundado na realização de um contrato. Este entendimento pode-se retirar de uma carta²⁹ do Comité Europeu para a Proteção de Dados, endereçada a Sophie in 't Veld, eurodeputada holandesa, que surge no seguimento de questões levantadas sobre a DSP2 pela mesma à Comissão e ao dito Comité Europeu para a Proteção de Dados³⁰.

A carta em resposta às questões levantadas pela eurodeputada holandesa conclui que, pese embora os dois diplomas utilizem a noção de “consentimento explícito”, a noção prevista no artigo 94.º, alínea 2 DSP2, deverá ser um consentimento contratual, distinta do entendimento previsto no RGD.

Constata-se, assim, que os dois diplomas compreendem noções em alguns pontos bastante distintas. Apesar de incluírem noções diferentes, estas não se destacam de forma alguma como algo prejudicial, uma vez que a importância de tais diferenças se revela mínima.

2.2. Dever de informação

Relativamente ao dever de informação, a DSP2 vem introduzir novas entidades. Nomeadamente, os Prestadores de Serviços de Informação sobre Contas (PSIC) e de Iniciação de Pagamentos (PSIP).

O primeiro³¹ materializa-se em o utilizador de serviços de pagamento ter acesso de forma agregada a informações sobre uma ou

²⁸ Cfr. artigo 64.º, alínea 4 DSP2.

²⁹ Carta de 5 de julho de 2018, disponível em https://edpb.europa.eu/sites/edpb/files/files/file1/psd2_letter_en.pdf.

³⁰ Carta de 16 de fevereiro de 2018, disponível em <https://www.sophieintveld.eu/question-marks-over-privacy-aspects-of-psd2-must-be-urgently-clarified/>.

³¹ Cfr. o ponto 19 do artigo 4.º, o considerando 28 e artigo 33.º da DSP2.

mais contas de pagamento de um ou mais prestadores de serviços de pagamento, através de interfaces *online*.

Já o segundo³² define-se na introdução do papel de intermediário nas compras online, sendo uma ponte entre o website do comerciante e a plataforma bancária online do prestador de serviços de pagamento, sem necessidade de haver uma relação contratual entre este e o prestador de serviço de pagamento.

No tocante às informações gerais, o prestador de serviços de pagamento fica obrigado a disponibilizar as referidas informações de forma acessível, facilmente compreensível, assim como clara e inteligivelmente, podendo estas, a pedido do utilizador, ser disponibilizadas em suporte papel ou outro duradouro³³.

Não obstante, a DSP2 prevê diversos requisitos de informações a prestar, consoante o destinatário³⁴. De um modo geral, é obrigatória a disponibilização de uma referência que permita às partes identificar a operação de pagamento ou o ordenante, o montante do pagamento e encargos que possam surgir com o mesmo, assim como a confirmação de que a iniciação da ordem de pagamento foi bem-sucedida.

Certo é que o RGPD prevê, de igual modo, certas informações que os titulares têm o direito de obter dos responsáveis pelo tratamento, nomeadamente informações da relação com o responsável³⁵ e informações que são tratadas por terceiros³⁶. Contudo, cabe ao terceiro comunicar que tratou dados pessoais do titular.

2.3. Dados pessoais

Atualmente, o RGPD é, indubitavelmente, o principal diploma a reger dados pessoais e a sua proteção. Não obstante o seu emparelhamento com os restantes diplomas europeus e nacionais, é recor-

³² Cfr. o ponto 18 do artigo 4.º e no considerando 27 da DSP2.

³³ Cfr. artigo 44.º DSP2.

³⁴ Cfr. artigos 44.º a 49.º e 56.º a 58.º DSP2.

³⁵ Cfr. artigo 13.º RGPD.

³⁶ Cfr. artigo 14.º RGPD.

rente os diplomas servirem-se de uma norma individual relativa a proteção de dados que acaba por remeter o regime para o RGPD.

É o que sucede com a DSP2 que, no seu artigo 94.º, regula a proteção de dados no tocante à Diretiva. O preceito permite que o tratamento de dados pessoais pelos sistemas de pagamento e pelos prestadores de serviços de pagamento ocorra quando “tal for necessário para salvaguardar a prevenção, investigação e deteção de fraudes em matéria de pagamentos”.

Nesse normativo, assim como no considerando 89, é referido que qualquer tratamento de dados pessoais para efeitos da DSP2 será efetuado nos termos da Diretiva 95/46/CE e da sua transposição e do Regulamento (CE) n.º 45/2001, que, agora revogados, deram lugar ao RGPD e ao Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados.

Assim como, no já mencionado considerando 89 da DSP2, é referido que “deverá ser especificado o objetivo exato, deverá ser referida a base jurídica aplicável (...) e deverão ser respeitados os princípios da necessidade, da proporcionalidade, da limitação da finalidade e do período proporcionado de conservação de dados”, espelhando a visão do RGPD. Inclusive, a proteção de dados desde a conceção e por defeito, prevista na parte final do dito considerando, é um dos pontos fundamentais do RGPD, previsto no seu artigo 25.º.

Do mesmo modo, é referido ainda que os PSP só acedem aos dados necessários para a prestação dos seus serviços e só os tratam e conservam com o devido consentimento expresse, seguindo a linha previamente exposta do RGPD no que toca ao consentimento e assumindo o princípio da limitação das finalidades³⁷ e da minimização³⁸

³⁷ Cfr. artigo 5.º, n.º 1, alínea b RGPD. Por princípio da limitação das finalidades entende-se que os dados pessoais são “recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades”.

³⁸ Cfr. artigo 5.º, n.º 1, alínea d RGPD. Por princípio da minimização dos dados entende-se que os dados pessoais são “adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados”.

e restantes princípios. Tais preceitos encontram o seu paralelo na DSP2, ao ser mencionado que o PSIP “não exige ao utilizador de serviços de pagamento quaisquer outros dados além dos necessários para prestar o serviço de iniciação do pagamento³⁹” e “não utiliza nem armazena dados nem acede aos mesmos para outros fins que não sejam a prestação do serviço de iniciação do pagamento expressamente solicitado pelo ordenante⁴⁰”.

É importante ressaltar que, ao abrigo das normas comunitárias, os utilizadores têm o direito de pedir para apagar os dados e as entidades a obrigação de o fazer, exceto nos casos ressaltados pelo legislador⁴¹.

Nomeadamente, os dados que o PSP possui serem necessários para exercer o direito à liberdade de expressão, quando uma obrigação jurídica obrigue a conservar os dados ou por motivos de interesse público, como investigações científicas⁴².

É certo que as entidades que tratem os dados devem tomar as devidas medidas para, por um lado, informar outras entidades de que a pessoa solicitou o apagamento e, por outro, que há meios para eliminar os dados pessoais⁴³. Este é um dado muito importante a reter, pois as autoridades nacionais têm sido implacáveis ao sancionar empresas justamente pela falta de implementação de medidas técnicas capazes.

Assim, também pelo entendimento da autoridade europeia de proteção de dados na carta suprarreferida, o artigo 94.º deverá servir de complemento ao RGPD e não em substituição de, devendo os PSP seguir o RGPD como base nas suas atuações.

³⁹ Cfr. artigo 66.º, n.º 3, alínea f DSP2.

⁴⁰ Cfr. artigo 66.º, n.º 3, alínea g DSP2.

⁴¹ Cfr. artigo 17.º RGPD. Este artigo prevê o “direito a ser esquecido”. Entendemos este um tópico de especial relevância, já com alguma literatura referente ao assunto. Destacamos Ana Perestrelo de Oliveira, *Direito ao apagamento dos dados ou “direito a ser esquecido” em Fintech: Novos Desafios da Tecnologia Financeira*, 1.ª edição, coord. António Menezes Cordeiro/Ana Perestrelo de Oliveira/Diogo Pereira Duarte, Almedina, 89-104.

⁴² Cfr. art. 17.º, n.º 3 RGPD.

⁴³ Cfr. considerando 65 e 66 e artigo 17.º RGPD.

3. Coimas

À data de redação do presente texto, embora não sendo com certeza um número final, há cerca de 350 registos⁴⁴ de coimas aplicadas por autoridades nacionais de proteção de dados a nível europeu, destacando-se as aplicadas à British Airways, no valor de €204.600.00, à Marriott International, no valor de €110.390.200 e à Google, no valor de €50.000.000.

Já no caso da Comissão Nacional de Proteção de Dados, destacando-se a coima aplicada ao Hospital do Barreiro, no valor de €400.000⁴⁵.

Ao abrigo do RGD, são previstas sanções pecuniárias até €20.000.000 ou até 4% do volume de negócios anual a nível mundial, caso se trate de uma empresa⁴⁶, consoante o que for mais elevado. Estas coimas poderão ser imputadas por violações dos direitos dos titulares ou dos princípios básicos de tratamento, incluindo as condições de consentimento, por exemplo.

Já a DSP2 dá a possibilidade de os Estados-Membros estabelecerem os seus regimes de sanções⁴⁷, sendo que o RJSPME prevê valores de coimas a ascender até €1.500.000, no caso de empresas, por violação de disposições presentes no diploma.

4. Conclusões

Aparenta haver, como acima explanado, uma falsa sensação de dicotomia inexata, tendo em conta que ambos os diplomas procuram fornecer aos clientes o controlo dos seus dados.

⁴⁴ Conforme a ferramenta elaborada pelo site de defesa da privacidade digital Privacy-Affairs.com, que agrupa as coimas impostas pelas autoridades de controlo europeias dos diversos Estados Membros. Consultado pela última vez a 21 de julho de 2020. Disponível em <https://www.privacyaffairs.com/gdpr-fines/>.

⁴⁵ Cfr. deliberação n.º 984/2018 da CNPD, relativa ao Processo n.º 9932/2018. Disponível em https://www.cnpd.pt/bin/decisoies/Delib/20_984_2018.pdf.

⁴⁶ Cfr. artigo 83.º, n.º 5 RGD.

⁴⁷ Cfr. artigo 103.º, n.º 1 DSP2.

No fundo, a adoção destes dois diplomas afigura-se vantajosa, uma vez que as inovações que daí decorrem, em especial a introdução dos TPP, possibilitam uma maior escolha no que toca a parceiros de serviços de pagamento.

Acima de tudo, quem beneficia é o consumidor, dado que assistimos a uma maior proliferação de soluções de segurança, ao crescimento de áreas associadas à inteligência artificial e, futuramente, a uma maior utilização e mesmo desenvolvimento de moeda virtual⁴⁸, levando a soluções automatizadas, mais eficientes e rentáveis.

Numa última nota, destaca-se a ausência, até ao momento em que escrevemos, de orientações ou diretrizes relativas aos assuntos que nos debruçámos ao longo do presente artigo, por parte das principais entidades portuguesas⁴⁹.

⁴⁸ Carlos Moura, *Fintech e regulação no mercado bancário em Fintech: Desafios da Tecnologia Financeira*, 2.^a edição, coord. António Menezes Cordeiro/Ana Perestrelo de Oliveira/Diogo Pereira Duarte, Almedina, 21-32, 21.

⁴⁹ Neste caso falamos das principais entidades reguladores e fiscalizadoras, como a Autoridade de Supervisão de Seguros e Fundos de Pensões, o Banco de Portugal, o Conselho Nacional de Supervisores Financeiros e a Comissão Nacional de Protecção de Dados.

Bibliografia

- Carlos Moura, Fintech e regulação no mercado bancário em Fintech: Desafios da Tecnologia Financeira, 2.^a edição, coord. António Menezes Cordeiro/Ana Perestrelo de Oliveira/Diogo Pereira Duarte, Almedina (2019)
- Patrick Schueffel. (2016). Taming the Beast: A Scientific Definition of Fintech. Acessível em SSRN: <http://papers.ssrn.com/abstract=3097312>, (consultado em 27 de março de 2020), 32-54

