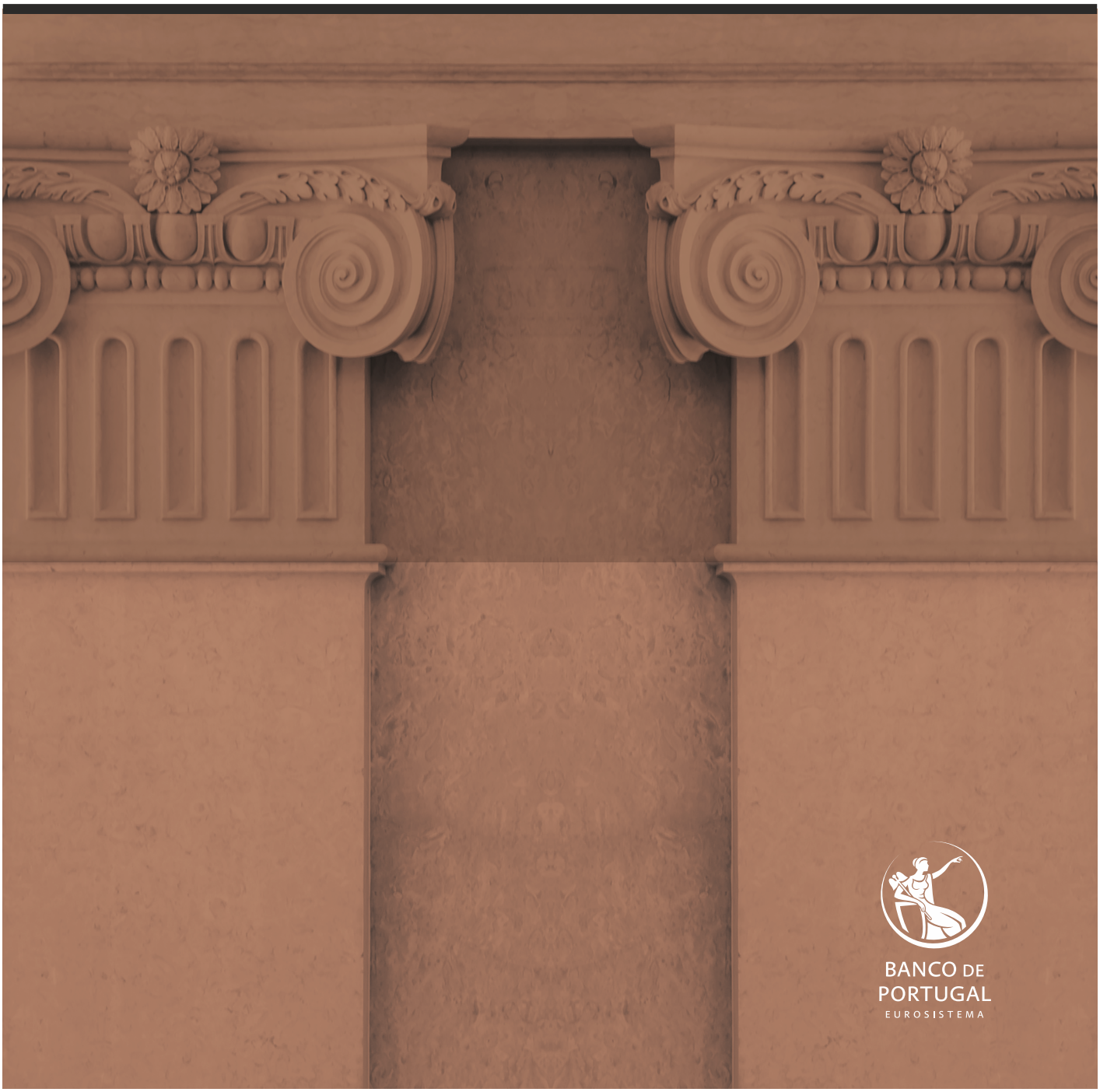
08

CADERNOS JURÍDICOS



BANCO DE PORTUGAL
EUROSISTEMA

8

CADERNOS JURÍDICOS

DEZEMBRO 2023

BANCO DE PORTUGAL
EUROSISTEMA

Lisboa, 2023 • www.bportugal.pt

Cadernos Jurídicos | Dezembro 2023 • Banco de Portugal Rua do Comércio, 148 | 1100-150 Lisboa • www.bportugal.pt
• Edição Departamento de Serviços Jurídicos • ISSN (*online*) 2184-5832

Índice

Nota de abertura

É com agrado que procedemos à publicação do oitavo número dos *Cadernos Jurídicos do Banco de Portugal*, dando seguimento à divulgação de estudos e de análises relativamente a questões jurídicas que, revestindo-se de particular atualidade e aplicação prática, se referem ao domínio das atribuições do Banco de Portugal ou a matérias com estas conexas.

Em particular, o presente número procede à publicação de um estudo, de um artigo científico e da anotação a um acórdão do Tribunal de Justiça da União Europeia, que se nos afigura contribuírem de forma relevante para a reflexão em torno dos temas em causa.

Desde logo, o artigo da autoria da Professora Doutora Maria Raquel Guimarães, docente na Faculdade de Direito da Universidade do Porto, apresenta uma análise das regras que regem a execução das ordens de pagamento, abordando as consequências resultantes da não autorização destas ordens pelo utilizador dos serviços de pagamento, num contexto que é caracterizado por uma acentuada evolução ao nível da prestação de serviços de pagamento, destacando-se a introdução de novas tecnologias que permitem a criação de instrumentos de pagamento "desmaterializados" e a consequente "mobilização dos serviços oferecidos". Tal suscita, de modo particular, a preocupação com a antecipação e a prevenção de operações fraudulentas por parte dos prestadores de serviços de pagamento.

Segue-se a publicação de estudo sobre os desafios jurídicos decorrentes do desenvolvimento e implementação de ferramentas de *RegTech* e *SupTech* no contexto da atividade de regulação e supervisão, da autoria da Dra. Luma Almeida e da Dra. Joana Gama Gomes, Juristas no Departamento de Serviços Jurídicos do Banco de Portugal. As Autoras analisam os referidos fenómenos sob a perspetiva do respetivo enquadramento normativo e dos principais benefícios e desafios suscitados neste âmbito. Antecipando-se que a utilização destas ferramentas venha a marcar decisivamente o funcionamento do setor bancário e financeiro, bem como as respetivas atividades de regulação e de supervisão, o presente estudo configura um contributo importante para uma compreensão e reflexão aprofundadas a este respeito.

O presente número conta ainda com a anotação, da autoria da Professora Doutora Isabel Alexandre, Jurista no Departamento de Serviços Jurídicos do Banco de Portugal, ao acórdão proferido pelo Tribunal de Justiça da União Europeia em 30 de novembro de 2021, no âmbito do Processo C-3/20. O acórdão em causa foi proferido no contexto de um reenvio a título prejudicial efetuado por um tribunal letão, perante o qual pendia um processo penal contra um antigo Governador do banco central da Letónia, por factos ocorridos durante o exercício destas funções. Neste contexto, o acórdão pronuncia-se sobre questões relativas à aplicação do regime de imunidade de jurisdição dos governadores de bancos centrais, destacando a anotação em causa as respetivas implicações práticas. Em anexo é disponibilizado, para benefício do leitor, excerto do acórdão anotado.

Assim, encontram-se reunidas, uma vez mais, as condições para proporcionar, a quem destes temas se ocupa ou para os quais dirige o seu interesse, uma estimulante leitura dos *Cadernos Jurídicos do Banco de Portugal*.

Luís Máximo dos Santos

Vice-Governador do Banco de Portugal

1 Serviços de pagamentos e instrumentos de pagamento

Maria Raquel Guimarães[1]

Abstract

Payment services have evolved significantly over the last decade, with the introduction of new technologies and the consequent mobilisation of payment instruments. With this scenario in mind, we will revisit the rules of the second Payment Services Directive with regard to contactless instruments, the requirement for strong user authentication, burden of proof, and new fraudulent transactions, namely social engineering schemes.

1 Introdução: serviços de pagamento e evolução tecnológica

Os serviços de pagamento são elencados no *Regime Jurídico dos Serviços de Pagamento e da Moeda Electrónica* (RSP 2), Anexo ao Decreto-Lei n.º 91/2018, de 12 de Novembro[2], de uma forma muito ampla, sem alusão às tecnologias utilizadas, abrangendo uma grande variedade de "operações de pagamento" — no sentido da sua alínea ii) do artigo 2.º —, como o depósito e levantamento de numerário, a execução de operações de pagamento mediante a transferência de fundos depositados ou a utilização de uma linha de crédito — incluindo débitos directos, operações de pagamento através de cartões e transferências a crédito —, bem como a emissão

[1] Professora Associada da Faculdade de Direito da Universidade do Porto; investigadora do CIJ — Centro de Investigação Jurídica (U.Porto) e do Grupo de Investigación Reconocido sobre Derecho de las Nuevas Tecnologias y Delincuencia Informática (U.Valladolid). O presente texto encontra-se publicado, com alterações de pormenor, com o título "Serviços de pagamento e instrumentos de pagamento: evoluções recentes", em *Estudos de direito do consumo*, volume II, Coimbra, Almedina, 2023, pp. 737–753, obra organizada por Rui Mascarenhas Ataíde, Francisco Rodrigues Rocha e Vítor Palmela Fidalgo, a quem se agradece a autorização para a sua republicação. Não se teve em consideração, na sua redacção, a 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, Bruxelas, COM(2023) 366 final, 28-6-2023, e 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) 367 final, Bruxelas, 28-6-2023, publicadas posteriormente.

[2] O RSP 2 veio transpor para o direito interno a Directiva (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 Directivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Directiva 2007/64/CE, *in JO* L 337/35, 23-12-2015 (DSP 2). Revogou o primeiro *Regime jurídico dos serviços de pagamento e da moeda electrónica* (RSP 1), incluído no Decreto-Lei n.º 317/2009 de 30 de Outubro — mais propriamente no seu Anexo I —, e alterado pelo Decreto-Lei n.º 242/2012, de 7 de Novembro. Por sua vez, o RSP 1 havia introduzido no direito nacional a Directiva 2007/64/CE do Parlamento Europeu e do Conselho, de 13 de Novembro de 2007, relativa aos serviços de pagamento no mercado interno, que altera as Directivas 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE e revoga a Directiva 97/5/CE, *in JO* L 319/1, 5-12-2007 (DSP 1, revogada, portanto, pela DSP 2) e a Directiva 2009/110/CE, do Parlamento Europeu e do Conselho, de 16 de Setembro, relativa ao acesso à atividade das instituições de moeda eletrónica, ao seu exercício e à sua supervisão prudencial, *in JO* L 267/7, 10-10-2009.

de instrumentos de pagamento, o envio de fundos e os serviços de *open banking* de iniciação de pagamentos e de informação sobre contas[3].

A actividade de prestação de serviços de pagamento tem evoluído de um modo significativo na última década, com a introdução de novas tecnologias, que permitem a criação de instrumentos de pagamento "desmaterializados", mais ágeis e cómodos, e com a consequente *mobilização* dos serviços oferecidos[4]. A *mobilização* dos serviços de pagamento leva a que as operações de pagamento sejam realizadas muitas vezes em redes públicas, através de dispositivos com pouca ou nenhuma capacidade para suportar actualizações de segurança, mediante a utilização de palavras-passe e códigos de acesso inseguros e até gravados no próprio dispositivo, onde aplicações de pagamento e sistemas de *homebanking* convivem com aplicações de redes sociais, jogos, e outras, muitas vezes de origem desconhecida e que funcionam como canais de recolha de dados pessoais.

Verificou-se, por outro lado, a abertura do mercado de pagamentos a prestadores de serviços não tradicionais, que operam com base em informações armazenadas por instituições financeiras ou bancárias, sobrepondo os seus serviços àqueles prestados por estas últimas, criando uma nova "camada" de serviços de pagamento "*over-the-top*" (OTT), hoje já abrangidos pela disciplina vigente dos serviços de pagamento[5]. Nas palavras expressivas do Banco de Portugal, "os bancos deixaram de ter o monopólio de dados sobre os seus clientes e foram obrigados a partilhá-los com novos prestadores de serviços de pagamento devidamente autorizados, o que tornou as contas bancárias numa espécie de 'matéria-prima', sobre a qual poderão ser desenvolvidos serviços inovadores"[6].

A utilização de novas tecnologias associadas a instrumentos de pagamento "clássicos" ou de novos instrumentos de pagamento, electronicamente mais sofisticados, para a realização de operações de pagamento à distância e presenciais, obrigam, porém, a repensar as medidas de segurança adoptadas. A intervenção do legislador europeu em 2015 e a subsequente intervenção do legislador nacional três anos mais tarde foram, em boa medida, motivadas por

[3] Cfr. o artigo 4.º do RSP 2, bem como as operações excluídas do seu âmbito de aplicação, enumeradas no artigo 5.º. Os serviços de iniciação de pagamento e de informação sobre contas são definidos nas alíneas *tt)* e *uu)* do artigo 2.º do RSP 2. Entre nós, para mais desenvolvimentos sobre os serviços de iniciação de pagamento, v. Patrícia Alexandra Paiva Duarte, "Os serviços de iniciação de pagamento no novo RSP", *in RED — Revista Electrónica de Direito*, vol. 25, n.º 2, Junho, 2021, p. 41 ss.

[4] O Banco de Portugal referiu-se em 2019 ao impacto da tecnologia nos serviços de pagamento como um "processo de disrupção tecnológica sem precedentes". *Vide* Banco de Portugal, *Relatório dos Sistemas de Pagamentos — 2019*, Lisboa, 2020, *in* <https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/rsp2019_0.pdf> (29-11-2023), p. 44 ss.

[5] Estes novos operadores no mercado dos serviços de pagamento começaram por prestar os seus serviços ao abrigo do princípio da liberdade contratual e sem a cobertura da lei, tendo a decisão de os abranger nas novas regras europeias dos serviços de pagamento sido considerada pela doutrina como uma das alterações mais significativas introduzidas em 2015 pela DSP 2 (cfr. os "considerandos" 27–29). Assim, Mª Nieves Pacheco Jiménez, "La nueva directiva 2015/2366 de servicios de pago en el mercado interior", *in Revista CESCO de Derecho de Consumo*, n.º 16/2016, p. 141, <https://revista.uclm.es/index.php/cesco> (29.11.2023); Mary Donnelly, "Payments in the digital market: Evaluating the contribution of Payment Services Directive II", *in Computer Law & Security Review*, n.º 32, 2016, pp. 829–832; Reinhard Steennot, "Reduced payer's liability for unauthorized payment transactions under second Payment Services Directive (PSD2)", *in Computer Law & Security Review*, n.º 34, 2018, pp. 954–956; Francisco Mendes Correia, "Uma revolução permanente? A DSP 2 e o novo direito dos serviços de pagamento", *in III Congresso de Direito Bancário*, L. Miguel Pestana de Vasconcelos (coord.), Coimbra, Livraria Almedina, 2018, pp. 388, 394–395; e 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. 143–144.

[6] Banco de Portugal, *Relatório dos Sistemas de Pagamentos — 2019*, cit., p. 44. Para mais desenvolvimentos sobre as questões de privacidade e segurança dos clientes que estes serviços colocam, sobretudo em virtude do processamento de dados bancários em larga escala, ver P.T.J Wolters/B.P.F Jacobs, "The security of access to accounts under PSD 2", *in Computer Law & Security Review*, n.º 35, 2019, pp. 29–41.

preocupações com a segurança[7]. Desde logo, visou-se reforçar a segurança dos serviços de pagamento oferecidos sobretudo por via electrónica e evitar a intromissão de terceiros com vista à realização de operações fraudulentas. E foi também intenção do legislador diminuir os riscos associados aos pagamentos fraudulentos a suportar pelo utilizador de serviços de pagamento, sempre que estas operações fraudulentas não possam ser evitadas.

Pretendemos neste texto abordar as regras que regem a execução das ordens de pagamento e as consequências que advêm da não autorização destas ordens pelo utilizador dos serviços de pagamento.

2 Instrumentos de pagamento e a funcionalidade *contactless*

A prestação de serviços de pagamento tem com frequência na sua base a utilização de um instrumento de pagamento, emitido em consequência da celebração de um contrato-quadro de utilização de um instrumento de pagamento. Este 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. Está, nesta medida, sujeito ao controlo de inclusão e ao controlo de conteúdo das suas cláusulas que decorre da aplicação do Decreto-Lei n.º 446/85, de 25 de Outubro. O legislador europeu, em 2015, chamou a atenção para os limites que se impõem às cláusulas contratuais gerais que integram os contratos de emissão e de utilização destes instrumentos de pagamento, dizendo que estas "têm de ser objetivas, não discriminatórias e proporcionais", tendo a mesma fórmula sido adoptada pelo legislador nacional em 2018[8].

O RSP 2 define instrumento de pagamento em termos muito latos, enquanto "*dispositivo personalizado ou conjunto de procedimentos acordados entre o utilizador e o prestador de serviços de pagamento e a que o utilizador de serviços de pagamento recorra para emitir uma ordem de pagamento*", ou seja, para desencadear "*o ato (...) de depositar, transferir ou levantar fundos, independentemente de quaisquer obrigações subjacentes entre o ordenante e o beneficiário*"[9]. Cabem nesta noção instrumentos muito díspares, onde se incluem os cartões de pagamento — "instrumentos de pagamento baseados em cartões"[10] —, de crédito ou de débito, mas também os procedimentos acordados para a realização de um pagamento através de *sites* de banca

[7] O reforço da segurança dos serviços de pagamentos, sobretudo realizados por via electrónica, é apontado como um dos desígnios da PSD 2 nos seus "considerandos" 95 e 96.

[8] Cfr. o artigo 69.º, n.º 1, alínea *a)*, da DSP 2 e o artigo 110.º, n.º 1, alínea *a)*, do RSP 2. Para mais desenvolvimentos sobre a caracterização deste contrato de utilização como um contrato de adesão, ver Maria Raquel Guimarães, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos*, Coimbra, Wolters Kluwer/Coimbra Editora, 2011, pp. 261–268.

[9] Cfr. as alíneas *aa)* e *ii)* do artigo 2.º do RSP 2.

[10] A noção de "instrumento de pagamento baseado em cartões" surge na alínea *bb)* do artigo 2.º do RSP 2.

electrónica, aplicações móveis, como o *MB Way*[11], mensagens de correio electrónico, e até procedimentos de emissão de ordens de pagamento através de formulários em papel[12].

O Tribunal Europeu de Justiça teve a oportunidade de se pronunciar no caso *T-Mobile Austria* no sentido da inclusão destes últimos procedimentos na noção de instrumentos de pagamento, tendo entendido que esta noção "é suscetível de cobrir um conjunto de procedimentos não personalizados, acordados entre o utilizador e o prestador de serviços de pagamento, aos quais o utilizador recorre para iniciar uma ordem de pagamento"[13], abrangendo, portanto, "a emissão de uma ordem de transferência mediante um formulário de transferência com a assinatura manuscrita do ordenante"[14].

Um mesmo dispositivo — como um computador ou um telemóvel — pode conter diferentes instrumentos de pagamento, tantos quantas as aplicações de pagamento que tenha instaladas ou aplicações de *home banking*[15]. Assim, impõe-se ao titular dos diferentes instrumentos de pagamento a sua utilização nos termos dos contratos-quadro respectivos, devendo ser tomadas "todas as medidas razoáveis" para preservar a segurança das credenciais e códigos que lhes estão associadas[16]. Do mesmo modo, em caso de perda ou extravio do dispositivo, impõe-se ao seu utilizador o dever de comunicar esse extravio, sem atraso injustificado, a cada um dos prestadores dos serviços de pagamento que emitiu os diferentes instrumentos de pagamento[17].

O mesmo instrumento de pagamento pode, por sua vez, incluir diferentes funcionalidades, como acontece nos cartões multifunções — nomeadamente de crédito e de débito —, definidas no contrato-quadro de utilização que gera a emissão do instrumento e fixa os termos da sua utilização[18].

O mesmo acontece com a função *contactless*, também identificada pela sigla NFC — *Near Field Communication* — que alguns cartões ou aplicações de telemóveis contêm. Esta funcionalidade incluída num instrumento de pagamento permite a realização de operações de pagamento sem a necessidade de outro elemento de autenticação do seu titular para além da aproximação do próprio cartão de um terminal de pagamento — portanto sem a autenticação forte que a lei exige, que analisaremos *infra* —, e está limitada a pagamentos até 50€ e até a um total acumulado de 150€ ou de cinco operações sucessivas, exigindo-se seguidamente a autenticação do titular, nomeadamente através da marcação de um PIN no terminal[19]. Trata-se de uma

[11] O *MB Way* é uma aplicação móvel, que se anuncia como "o Multibanco no telemóvel", e permite, entre outras operações, "espelhar" um cartão de débito no telemóvel a fim de realizar pagamentos *contactless* em terminais de pagamento electrónico, transferir e receber fundos para/de outros dispositivos móveis, e gerar códigos — enviados por SMS — que, associados a um número de telefone móvel, permitem o levantamento de numerário directamente em caixas automáticas. Cfr. https://www.mbway.pt/, (29-11-2023).

[12] Assim, Reinhard Steennot, "Liability for unauthorized payment transactions: the transposition of PSD2 in Belgium", *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, p. 175, e Maria Raquel Guimarães/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, § 14.

[13] TJUE, Processo C-616/11, *T-MobileAustria*, 9 de Abril de 2014, ECLI:EU:C:2014:242, § 35. O Tribunal apreciou a noção de "instrumento de pagamento" à luz da Directiva 2007/64/CE (PSD 1), que previa uma noção idêntica à consagrada na DSP 2. Cfr. § 29 ss., em especial §§ 38, 41, 44.

[14] *Idem*, § 38.

[15] Maria Raquel Guimarães/Reinhard Steennot, "Allocation of liability in case of payment fraud...", cit., § 15.

[16] Cfr. o artigo 110.º, n.º 1, alínea *a)*, e n.º 2, do RSP 2.

[17] Cfr. o artigo 110.º, n.º 1, alínea *b)*, do RSP 2.

[18] Sobre os cartões *multifunções* ou *multifuncionais*, v. o nosso *As transferências electrónicas de fundos e os cartões de débito. Alguns problemas jurídicos relacionados com as operações de levantamento de numerário e de pagamento por meios electrónicos*, Coimbra, Livraria Almedina, 1999, pp. 64–65.

[19] Cfr. o artigo 11.º do Regulamento Delegado (UE) 2018/389 da Comissão de 27 de Novembro de 2017 que complementa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras, *in JO* L 69, 13-03-2018, pp. 23–43.

funcionalidade incorporada num instrumento de pagamento, que o titular pode escolher utilizar ou não em cada operação, e não de um novo instrumento de pagamento distinto do instrumento de pagamento em que está incorporada.

Nesta medida, não podemos seguir a posição adoptada pelo Tribunal Europeu de Justiça no caso *DenizBank*, e apoiada pelas conclusões advogado-geral, segundo a qual "a utilização da função NFC de um cartão bancário associado a uma conta bancária individual 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"[20].

A função NFC ou "sem contacto" não corresponde a um instrumento de pagamento *ad hoc* mas, como dissemos, a uma funcionalidade incluída nalguns instrumentos de pagamento que permite aligeirar a autenticação do utilizador em determinadas operações, com limites de valores e de frequência de utilização. A natureza do instrumento de pagamento é estabelecida no contrato-quadro bem como as utilizações que suporta, nomeadamente uma utilização *contactless*. E a natureza do instrumento de pagamento não muda ao fim de cada cinco operações sucessivas ou em função do valor do pagamento ou do valor acumulado de pagamentos, nem sequer o instrumento de pagamento pode ser considerado de forma intermitente como um "instrumento de baixo valor", para efeitos de aplicação das derrogações do artigo 102.º, n.º 1, dependendo do valor de cada pagamento realizado[21]. A não ser assim, teríamos que considerar que também os cartões multifuncionais incorporam diferentes instrumentos de pagamento e mesmo um cartão de crédito, que pode ser utilizado presencialmente, com a marcação de um código secreto num terminal de pagamento, e à distância, mediante a indicação do nome do titular, número, e data de validade, acrescidos de um código gerado para a operação em causa e enviado para um dispositivo móvel, incorporaria dois instrumentos de pagamento distintos, consoante a modalidade de utilização[22].

Desde logo, seguindo as considerações do TJUE, o prestador de serviços de pagamento incumpriria a sua obrigação de não enviar um instrumento de pagamento não solicitado ao utilizador sempre que substituísse um cartão de pagamento sem função *contactless* por outro que incorporasse essa função, uma vez que lhe estaria a enviar um novo instrumento de pagamento[23].

[20] TJUE, Processo C-287/19, *DenizBank AG*, 11 de Novembro de 2020, ECLI:EU:C:2020:897, § 75.

[21] Maria Raquel Guimarães/Reinhard Steennot, "Allocation of liability in case of payment fraud...", cit., § 50.

[22] *Idem*, § 16.

[23] Cfr. o artigo 111.º, n.º 1, alínea *b)*, do RSP 2. Assim, Maria Raquel Guimarães/Reinhard Steennot, "Allocation of liability in case of payment fraud...", cit., § 17.

3 Autenticação forte do utilizador de serviços de pagamento

O RSP 2 exige que a autenticação do utilizador dos serviços de pagamento necessária para autorizar uma operação de pagamento electrónica seja uma autenticação *forte*[24], 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*"[25].

No seu artigo 104.º, n.º 2, o RSP 2 estipula ainda que nas operações de pagamento "remotas" a autenticação forte do cliente terá que incluir "*elementos que associem de forma dinâmica a operação a um montante específico e a um beneficiário específico*"[26]. Para estas operações à distância a lei não se basta já com uma autenticação baseada em dois elementos distintos e exige uma ligação "dinâmica" entre os elementos de autenticação exigidos e a operação de pagamento, o seu montante e o seu beneficiário. Pretende-se reforçar os mecanismos de identificação do utilizador dos serviços de pagamento que emite uma ordem de pagamento à distância, nomeadamente através de uma operação de banca electrónica ou mediante a utilização de um cartão de pagamento *online* e, nesta medida, aumentar a confiança no comércio electrónico e nas operações de pagamento à distância.

O Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de Novembro de 2017, prevê, porém, a possibilidade de isenção dos requisitos de autenticação forte em algumas situações, como no caso dos pagamentos *contactless*, nos termos já apontados, e das operações de pequeno valor "remotas"[27], ou ainda dos pagamentos a favor de "beneficiários fiáveis", devidamente credenciados, ou de operações recorrentes[28], justificadas pelo menor risco que apresentam[29].

O reforço dos requisitos de autenticação do utilizador de serviços de pagamento surge acompanhado no RSP 2 de novas soluções em matéria de pagamentos não autorizados, no sentido de incentivar a utilização de tecnologia mais segura por parte dos prestadores de serviços de pagamento e de promover a confiança dos seus utilizadores, favorecendo o mercado de pagamentos electrónicos.

[24] Cfr. o artigo 104.º, n.º 1, do RSP 2; os artigos 4.º, n.º 1, e 5, n.º 1, do Regulamento Delegado (UE) 2018/389 da Comissão de 27 de Novembro de 2017; e artigo 97.º, n.º 1, da DSP 2.

[25] Cfr. o artigo 2.º, alínea *d)*, do RSP 2.

[26] Ver também o artigo 97.º, n.º 2 da DSP 2. São operações de pagamento "remotas" as operações de pagamento iniciadas "*através da Internet ou através de um dispositivo que possa ser utilizado para comunicação à distância*:" artigo 2.º, alínea *kk)*, do RSP 2; e artigo 4.º, n.º 6, da DSP 2.

[27] Conforme dissemos *supra*, esta isenção de autenticação forte para as operações *contactless* está limitada aos pagamentos até 50 € e até a um total acumulado de 150 € e de cinco operações sucessivas. No caso das operações "remotas" de pequeno valor, a isenção até limitada aos pagamentos até 30 € e ao montante acumulado de 100 € e de cinco operações sucessivas. Cfr. os artigos 11.º e 16.º do referido Regulamento.

[28] Cfr. os artigos 13.º e 14.º do Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de Novembro de 2017.

[29] Cfr. os "considerandos" 9–12 do Regulamento Delegado (UE) 2018/389.

4 Operações fraudulentas de pagamento não autorizadas: pagamentos *contactless*, fraude não detectável, extravio do instrumento de pagamento e obrigações das partes

O disposto em matéria de requisitos de autenticação do utilizador para a realização de pagamentos electrónicos leva a que o RSP 2 venha consagrar que "*[s]e o prestador de serviços de pagamento do ordenante não exigir a autenticação forte do ordenante, este não deve suportar quaisquer perdas relativas a operação de pagamento não autorizada, salvo se tiver agido fraudulentamente*"[30]. Acrescenta-se ainda que caso "*o beneficiário ou o seu prestador de serviços de pagamento não aceite a autenticação forte do cliente, reembolsa os prejuízos financeiros causados ao prestador de serviços de pagamento do ordenante*"[31].

Assim, as perdas resultantes das operações de pagamento realizadas fraudulentamente por um terceiro *online*, sem autenticação "dinâmica", mediante a mera indicação dos dados impressos num cartão de crédito ou de débito — nome, número do cartão, data de validade, código de verificação —, ou das transferências não autorizadas efectuadas através da banca electrónica, inserindo apenas o código secreto do titular da conta e uma ou mais coordenadas impressas num cartão-matriz — que têm frequentemente ocupado os nossos tribunais[32] —, nunca serão suportadas pelo titular do cartão ou da conta a menos que este tenha actuado de modo fraudulento, o que equivale a dizer que o prestador do serviço terá que fazer prova desta actuação fraudulenta para imputar as perdas sofridas ao seu cliente[33]. Em todas as demais situações, será o prestador dos serviços de pagamento que arcará com as consequências de não exigir uma autenticação "qualificada", "dinâmica", do seu cliente — ou seja, de não investir em mecanismos de autenticação mais seguros —, a menos que a inexigência de uma autenticação "qualificada" seja devida ao beneficiário de pagamento ou ao seu prestador de serviços de pagamento, hipótese em que serão estes a suportar os prejuízos, como dissemos *supra*.

Também nos casos em que a inexistência de uma autenticação forte se verifica a coberto da lei, como acontecerá nos pagamentos *contactless* dentro dos limites de valores fixados pelo artigo

[30] Cfr. o artigo 115.º, n.º 5, do RSP 2 e o artigo 74.º, n.º 2, da DSP 2. Defendíamos já esta solução à luz do regime de 2009, entretanto revogado, embora não resultasse expressamente da redacção da lei, que não tratava directamente a questão: "(Ainda) a responsabilidade pelo uso indevido de instrumentos de pagamento electrónicos em operações presenciais e à distância, Análise do regime introduzido pelo Anexo I do Decreto-Lei n.º 317/2009, de 30 de Outubro (RSP), e das alterações que se perspectivam face à Proposta de Directiva do Parlamento Europeu e do Conselho, de 24 de Julho de 2013", *in I Congresso de Direito Bancário*, L. Miguel Pestana de Vasconcelos (coord.), Coimbra, Livraria Almedina, 2015, pp. 133–139, e em "A fraude no comércio electrónico: o problema da repartição do risco por pagamentos fraudulentos", *in Infracções Económicas e Financeiras: Estudos de Criminologia e de Direito*, José Neves Cruz, Carla Cardoso, André Lamas Leite, Rita Faria (coords.), Coimbra, FDUP/Coimbra Editora, 2013, pp. 592–594.

[31] Cfr. o artigo 115.º, n.º 6, do RSP 2.

[32] Para uma análise da jurisprudência nacional que tem apreciado as operações não autorizadas de banca electrónica realizadas com recurso a um cartão-matriz, ver Maria Raquel Guimarães, "O *phishing* de dados bancários e o *pharming* de contas. Análise jurisprudencial", *in III Congresso de Direito Bancário*, L. Miguel Pestana de Vasconcelos (coord.), Coimbra, Livraria Almedina, 2018, pp. 405–432, Patrícia Guerra, "A realização de operações de pagamento não autorizadas e a tutela do utilizador de serviços de pagamento em face do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica", *in RED — Revista Electrónica de Direito*, n.º 2, Junho, 2016, pp. 43–50, e Raquel Sofia Ribeiro de Lima, "A responsabilidade pela utilização abusiva *on-line* de instrumentos de pagamento eletrónico na jurisprudência portuguesa", *in RED — Revista Electrónica de Direito*, n.º 3, Outubro, 2016, p. 29 ss.

[33] Haverá nomeadamente uma actuação fraudulenta do utilizador do serviço de pagamento quando foi ele próprio o autor das operações que imputa a um terceiro ou quando este terceiro é um seu cúmplice no esquema fraudulento.

11.º do Regulamento Delegado (UE) 2018/389, o utilizador do instrumento de pagamento não suportará quaisquer prejuízos decorrentes de operações não autorizadas. A lei não prevê a derrogação desta regra para estas situações e nem sequer a qualificação, muito discutível, dos instrumentos *contactless* como "instrumentos de pagamento de baixo valor" utilizados "de forma anónima" — para os efeitos da alínea *b)* do n.º 1 do artigo 102.º do RSP 2 — confere a possibilidade do disposto no artigo 115.º, n.º 5, ser afastado contratualmente[34]. Nesta medida, terá que ser o prestador de serviços de pagamento a suportar o risco da utilização não autorizada dos instrumentos de pagamento *contactless*, risco esse que será certamente compensado pelo aumento da utilização destes instrumentos, potenciado pela facilidade e simplicidade que lhes está associada[35]. Só assim se cumpre o propósito do legislador europeu de "permitir o desenvolvimento de meios de pagamento acessíveis e de fácil utilização para pagamentos de baixo risco, como, por exemplo, os pagamentos de baixo valor através de tecnologia de leitura por aproximação (*contactless*), sejam eles baseados num telemóvel ou não"[36]. Esta foi também a posição assumida expressamente pela Autoridade Bancária Europeia (EBA — *European Banking Authority*) no seu *Single Rulebook* quando questionada sobre quem deveria arcar com os prejuízos em caso de operações isentas de autenticação forte levadas a cabo fraudulentamente[37]. No mesmo sentido teve a oportunidade de se pronunciar igualmente o Banco de Portugal[38].

Não obstante, o Tribunal Europeu de Justiça, no caso *DenizBank*, afirmou, sem mais desenvolvimentos, que se "deve considerar que um cliente que escolheu beneficiar de um instrumento de pagamento simplificado e sem necessidade de identificação para os pagamentos de baixo valor, como a função NFC, aceitou ficar eventualmente exposto aos efeitos das limitações convencionais da responsabilidade do prestador que são permitidas ao abrigo desta disposição", sem deixar claro que a regra da não imputação de prejuízos ao utilizador quando não tenha havido autenticação forte não admite derrogações contratuais e não se encontra incluída no leque de limitações convencionais previstas para os pagamentos de baixo

[34] Esta qualificação foi adoptada pelo TJUE, no caso *DenizBank AG* já referido, §§ 89–93. No entanto, parece-nos que o TJUE considerou, indevidamente, como já defendemos *supra*, que a função "sem contacto" do cartão de pagamento constituía um instrumento de pagamento *autónomo* em relação ao instrumento de pagamento "personalizado" em que o cartão se traduz. E considerou que este segundo instrumento de pagamento "de baixo valor" seria um instrumento "não personalizado" e, portanto, de "utilização anónima", permitindo que "qualquer pessoa que tenha acesso ao referido cartão po[ssa] efetuar [um] pagamento, dentro do limite máximo autorizado, incluindo sem o consentimento do titular da conta, em caso de perda, furto ou apropriação indevida do cartão" (§ 87). No entanto, os cartões de pagamento com uma função *contactless* não se transformam em títulos ao portador para os efeitos específicos da realização de cinco pagamentos até 50 € e com o limite acumulado de 150 €, e se, de facto, é possível levar a cabo pagamentos sem autenticação forte, isso não significa que a actuação não autorizada de um terceiro seja lícita, tal como ocorre com a realização de pagamentos *online* mediante a simples indicação dos dados impressos num cartão de pagamento, uma vez que este terceiro não é o titular do cartão. A simplificação, dentro dos limites definidos, da autenticação do titular do instrumento de pagamento não interfere com a sua natureza, como, de resto, resulta claramente do Regulamento Delegado (UE) 2018/389, que distingue, para efeitos da isenção de autenticação forte, as hipóteses de "pagamentos sem contacto no ponto de venda" (artigo 11.º) e de "operações de pequeno valor" (artigo 16.º), cujos valores máximos são, inclusive, distintos: 50 € e 30 €, respectivamente [artigo 102.º, n.º 1, do RSP 2 e artigos 11.º e 16.º do Regulamento Delegado (UE) 2018/389]. Sobre o tema, no sentido aqui defendido, v. Maria Raquel Guimarães /Reinhard Steennot, "Allocation of liability in case of payment fraud…", cit., §§ 39, 49, 50.

[35] De acordo com os dados apresentados pelo Banco de Portugal, a adopção generalizada da tecnologia *contactless* foi "um dos efeitos mais claros da pandemia nos pagamentos", levando a um aumento do número de operações em 163% e ao aumento do seu valor em 271%, relativamente ao ano de 2019: Banco de Portugal, *Relatório dos Sistemas de Pagamentos — 2020*, Lisboa, 2021, *in* https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/rsp2020.pdf, (29-11-2023), p. 18.

[36] Cfr. o "considerando" 96 da DSP 2.

[37] EBA, *Single Rulebook Q&A*, Topic "Strong customer authentication and common and secure communication (incl. access)", question 2018_4042: "Unless the payer acted fraudulently, the payer's PSP is liable towards that payer for transactions carried out without SCA. If the PSP of the payee triggers an SCA exemption and the transaction is carried out without an SCA, the payee's PSP will be liable towards the payer's PSP for the financial damage caused", *in* https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4042, (29-11-2023).

[38] Banco de Portugal, *Relatório dos Sistemas de Pagamentos — 2019*, cit., p. 41.

valor[39]. Ainda que não tenha posto em causa a aplicação do disposto no n.º 2 do artigo 74.º da DSP 2 — e n.º 5 do artigo 115.º do nosso RSP 2 — no caso dos pagamentos "sem contacto", o Tribunal Europeu veio, desnecessariamente, introduzir alguma perturbação na interpretação do preceito.

Nas situações em que a operação fraudulenta de pagamento é realizada com autenticação forte do ordenante, ou autenticação forte "qualificada", sempre que a lei a exige, e resulta do "extravio" do instrumento de pagamento — a lei refere-se à perda, furto, roubo ou a apropriação abusiva de um instrumento de pagamento[40] —, o risco assumido pelo titular do instrumento de pagamento foi reduzido pelo RSP 2 para 50 euros, ainda que não lhe seja imputável qualquer negligência pelo ocorrido[41]. Prevê-se, porém, um agravamento deste valor até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento para os casos em que tenha havido negligência grosseira do seu titular[42]. Não distingue a lei, também aqui, consoante o tipo de instrumento de pagamento utilizado para levar a cabo a operação não autorizada, podendo este ser um cartão de débito, crédito, um sistema de *homebanking*, ou telemóvel com uma aplicação associada, ou outro dispositivo semelhante.

Se o extravio do instrumento de pagamento não puder ser detectado pelo utilizador antes da realização de uma operação não autorizada — porque o instrumento de pagamento se encontra na sua posse, bem como os demais dispositivos de segurança que lhe estejam associados, como um telemóvel para onde são enviados os códigos dinâmicos necessários às operações ou *tokens* que geram códigos para cada operação individual —, nomeadamente em resultado de contratos *online*, sem a utilização "física" do instrumento de pagamento ou como consequência da "duplicação" deste instrumento ou da sua corrupção por via informática, o seu titular já não assumirá qualquer prejuízo pelas operações não autorizadas[43].

Em qualquer das hipóteses de constatação de uma operação não autorizada ou do extravio do instrumento de pagamento, impõe-se, desde logo, ao utilizador a comunicação desses factos, "*logo que [deles] tenha conhecimento*" e "*sem atraso injustificado*", ao prestador dos serviços de pagamento ou à entidade designada no contrato de utilização do instrumento de pagamento[44].

Acresce que a lei impõe ao prestador dos serviços de pagamento o dever de reembolsar *imediatamente* o seu cliente no montante da operação de pagamento não autorizada, logo que esta lhe tenha sido comunicada ou que, *independentemente desta comunicação*, *dela tenha tido conhecimento* — conforme se acrescentou na revisão do regime, na linha dos deveres de

[39] TJUE, Processo C–287/19, *DenizBank AG*, 11 de Novembro de 2020, cit., § 91.

[40] Cfr. o n.º 1 do artigo 115.º do RSP 2. Esta hipótese poderá resultar da perda ou furto de um telemóvel através do qual se assegura a recepção dos códigos dinâmicos gerados para cada operação ou do seu acesso por um terceiro através de um *software* malicioso, associados a um esquema de *phishing* pelo qual são obtidas as credenciais de acesso a uma determinada conta bancária *online* ou aplicação de pagamento.

[41] Cfr. o n.º 1 do artigo 115.º do RSP 2. No artigo 72.º, n.º 1, do anterior regime, o RSP 1, previa-se um montante de 150 euros, para circunstâncias idênticas, ainda que para a hipótese de apropriação abusiva de um instrumento de pagamento se exigisse a "*quebra da confidencialidade dos dispositivos de segurança personalizados imputável ao ordenante*", pressupondo o incumprimento dos seus deveres de cuidado.

[42] Cfr. o n.º 4 do artigo 115.º do RSP 2. Acrescenta-se ainda que, nos termos do n.º 3 deste artigo, "*o ordenante suporta todas as perdas resultantes de operações de pagamento não autorizadas, se aquelas forem devidas a atuação fraudulenta ou ao incumprimento deliberado de uma ou mais das obrigações previstas no artigo 110.º, caso em que não são aplicáveis os limites referidos no n.º 1*". Sobre a responsabilidade contratual do utilizador nestas hipóteses, ver Mafalda Miranda Barbosa, "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), n.º 1, p. 669, 22-11-2017, https://www.revistadedireitocomercial.com, (29-11-2023).

[43] Cfr. a alínea *a)* do n.º 2 do artigo 115.º do RSP 2. A mesmo solução está prevista para os casos em que as perdas são imputáveis a um trabalhador ou a um agente do prestador do serviço de pagamento (alínea *b)*). Sobre o âmbito de aplicação da primeira hipótese referida, e questionando sobre quem recai o ónus da prova da susceptibilidade da operação não autorizada ser detectável, v. Mary Donnelly, "Payments in the digital market…", cit., p. 835, e Reinhard Steennot, "Reduced payer's liability for unauthorized payment transactions…", cit., p. 962.

[44] Cfr. a alínea *b)*, n.º 1 do artigo 110.º do RSP 2.

monitorização impostos ao prestador de serviços de pagamento[45]. Esclarece ainda o legislador que "*em todo o caso*", este reembolso deverá ser feito "*o mais tardar até ao final do primeiro dia útil seguinte àquele conhecimento ou comunicação*"[46]. Esta obrigação de reembolso imediato apenas cederá, de acordo com o n.º 2 do artigo 114.º, quando o prestador do serviço de pagamento "*tiver motivos razoáveis para suspeitar de atuação fraudulenta do ordenante e comunicar por escrito esses motivos, no prazo indicado no número anterior, às autoridades judiciárias nos termos da lei penal e de processo penal*"[47].

As regras fixadas para a distribuição das perdas pelas partes nos contratos de utilização de instrumentos de pagamento apenas se aplicam, porém, a operações não autorizadas levadas a cabo *antes* da comunicação ao prestador de serviços do extravio do instrumento de pagamento ou da sua utilização não autorizada. É sobre a instituição prestadora do serviço de pagamento que a lei faz recair a obrigação de "*impedir qualquer utilização do instrumento de pagamento logo que a comunicação prevista na alínea b) do n.º 1 do artigo 110.º tenha sido efetuada*"[48] uma vez que é esta que dispõe de todos os meios técnicos necessários para impedir a sua posterior utilização, quer no país onde foi emitido quer no estrangeiro. Assim, justifica-se que seja esta entidade prestadora de serviços de pagamento que responda pelos prejuízos resultantes de operações não autorizadas levadas a cabo *posteriormente* à comunicação do "extravio" do instrumento de pagamento realizada pelo titular respectivo[49].

5 "Engenharia social" e operações fraudulentas de pagamento facilitadas ou autorizadas pelo utilizador

Muitos dos esquemas fraudulentos levados a cabo com vista à realização de operações de pagamento em benefício de terceiros são realizados com a "colaboração" activa do próprio utilizador do serviço de pagamento (APP — *Authorised Push Payments*), que é induzido, através de métodos de "engenharia social", a participar na sua própria decepção[50].

[45] Sobre esta imposição de um comportamento activo e não meramente reactivo ao prestador de serviços de pagamento, no sentido de tomar a iniciativa do reembolso detectada uma operação não autorizada, independentemente da comunicação do seu cliente, ver Mary Donnelly, "Payments in the digital market...", cit., p. 834; e Maria Raquel Guimarães, "The transposition of PSD2...", cit., p. 151, nota 33. Quanto aos deveres de monitorização que se impõem ao prestador do serviço, ver Maria Raquel Guimarães/Reinhard Steennot, "Allocation of liability in case of payment fraud...", cit., §§ 52–56, e Maria Raquel Guimarães, "Pagamentos electrónicos não autorizados e fraudulentos", *in Cibercriminalidade: novos desafios, ofensas e soluções*, Inês Sousa Guedes e Marcus Alan de Melo Gomes (Eds.), Lisboa, Pactor — Edições de Ciências Sociais, Forenses e da Educação, 2021, pp. 237–238.

[46] Cfr. o artigo 114.º, n.º 1, do RSP 2.

[47] Em todos os demais casos, o não cumprimento deste dever de reembolso acarreta a obrigação de pagamento de "*juros moratórios, contados dia a dia desde a data em que o utilizador de serviços de pagamento tenha negado que autorizou a operação de pagamento executada, até à data do reembolso efetivo da mesma, calculados à taxa legal, fixada nos termos do Código Civil, acrescida de 10 pontos percentuais, sem prejuízo do direito à indemnização suplementar a que haja lugar*". Cfr. o n.º 10 do artigo 114.º do RSP 2.

[48] Cfr. a alínea *e)* do n.º 1 do artigo 111.º do RSP 2.

[49] Cfr. o n.º 7 do artigo 115.º do RSP 2. Excepcionam-se, também aqui, os casos de actuação fraudulenta do próprio titular. No sentido de estarmos aqui perante um caso de responsabilidade por culpa do prestador do serviço, ver Mafalda Miranda Barbosa, "Serviços de pagamentos, repartição do risco e responsabilidade civil...", cit., pp. 674–675.

[50] European Payments Council, *2019 Payment Threats and Fraud Trends Report*, EPC302-19/Version 1.0/Date issued: 9 December 2019, *in* https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2019-12/EPC302-19%20v1.0%202019%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf (29-11-2023), p. 17. Seguimos aqui o que dissemos sobre o tema em "Pagamentos electrónicos não autorizados e fraudulentos", cit., pp. 228–229.

Estes métodos de "engenharia social" podem ser levados a cabo através de qualquer meio de telecomunicação, desde logo pelo telefone, correio electrónico, SMS, redes sociais, com vista a obter as credenciais que permitem o acesso ao serviço de pagamento (*phishing*) ou induzir o utilizador a realizar ele próprio um pagamento indevido. A vítima é aliciada através de investimentos falsos, compras ou vendas fantasma, negócios com lucros fáceis, ou de relações românticas. Ou ainda, é criada uma situação de medo face a um iminente ataque a uma conta *online*, sendo a vítima induzida a revelar as suas credenciais de acesso a um falso funcionário do banco para evitar a fraude[51].

Os esquemas de "engenharia social" têm evoluído rapidamente nos últimos tempos, sobretudo aproveitando a situação de confinamento provocada pela crise pandémica e uma maior propensão para "viver *online*", tendo sido considerados como uma das mais importantes ameaças à segurança dos pagamentos no ano de 2020 pelo *European Payments Council*[52].

Entre nós, estes métodos têm sido ultimamente utilizados em operações fraudulentas realizadas com recurso à aplicação de pagamento móvel *MB Way*, desencadeando, em muitos casos, pagamentos autorizados pelo utilizador do serviço móvel ou, pelo menos, levados a cabo em consequência do acesso que este faculta ao serviço.

Os esquemas fraudulentos mais frequentes surgem em resposta a um anúncio de venda de um bem em segunda mão numa plataforma electrónica, visando enganar o vendedor (ou é o próprio terceiro que se anuncia como vendedor de um bem na plataforma electrónica, visando enganar o comprador). Numa primeira modalidade de fraude, a vítima é instruída através de uma conversa telefónica para instalar a aplicação *MB Way* no seu telefone com recurso a uma caixa automática ou, sendo já utilizadora, para efectuar ou receber o pagamento devido, consoante o caso. Depois de inserir o seu cartão de débito e o seu código na caixa automática, é-lhe dito para inserir o número de telefone do falso comprador e o PIN indicado por este, recebendo ele no seu telefone o código de acesso à aplicação *MB Way*. Em alternativa, é inserido o número de telefone do utilizador (que o terceiro conhece porque este lhe foi facultado precisamente para acordarem o pagamento) e o código indicado pelo terceiro, e é pedido ao utilizador o código de verificação recebido por SMS. Em qualquer dos casos, o utilizador está a dar acesso ao terceiro à sua conta bancária, ainda que sem a consciência de o fazer, e não obstante as mensagens que são exibidas em janela durante o processo de adesão no sentido de nunca associar um número de telefone de um terceiro à aplicação e de não facultar o PIN de acesso ao serviço a outras pessoas. Não se trata, nesta medida, exactamente de um "extravio" do instrumento de pagamento nos mesmos moldes que acontecem nos casos de *phishing* "tradicionais" levados a cabo em serviços de *homebanking*, uma vez que o terceiro não acede aos códigos de segurança do utilizador mas antes são criados novos códigos de acesso ao serviço indicados pelo terceiro. Ainda assim, poder-se-á defender que há um "extravio" das novas credenciais de segurança do instrumento de pagamento, para efeitos do artigo 115.º, n.º 1, do RSP 2, alteradas inconscientemente pelo titular.

Nestas hipóteses, os prejuízos resultantes das operações que venham a ser realizadas pelo terceiro, de levantamento de numerário ou de transferência de fundos, recairá sobre o utilizador que lhe facultou o acesso à sua conta, na medida em que tenha adoptado um comportamento contrário ao expressamente indicado — de forma adequada e eficaz — pelo prestador dos

[51] European Payments Council, *2019 Payment Threats and Fraud Trends Report*, cit., pp. 80–81.

[52] European Payments Council, *2019 Payment Threats and Fraud Trends Report*, cit., p. 38. Para uma visão da tipologia que estes esquemas "APP" podem apresentar, ver UK Finance, *Fraud — The Facts 2021, The definitive overview of payment industry fraud*, 2021, *in* https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf (29-11-2023), pp. 52–73.

serviços de pagamento e, assim, tenha actuado com negligência grosseira, nos termos do art. 115.º, n.º 4, do RSP2.

A montante desta solução está, portanto, o cumprimento por parte do prestador do serviço de pagamento dos seus deveres de informação no sentido de facultar ao seu cliente a descrição das medidas que este deve adoptar para preservar a segurança do seu instrumento de pagamento. A não se considerarem cumpridos estes deveres de informação, e havendo sempre que apreciar a conduta do utilizador atendendo às particularidades do caso concreto, a este utilizador não poderia, em princípio, ser imputado um juízo de censura para além da negligência leve, com as consequências do n.º 1 do art. 115.º, do RSP 2: suportar perdas até 50 euros.

Uma segunda categoria de operações fraudulentas tem na sua base um esquema ainda mais simples de actuação: no momento em que o utilizador deveria receber um pagamento do terceiro via *MB Way*, para quitação do preço de um bem vendido na sequência de um anúncio numa plataforma electrónica, é instruído, também telefonicamente, para "enviar dinheiro" ao falso comprador em vez de lhe "pedir dinheiro" (ou para aceitar um pedido de dinheiro em vez de um pagamento). Nestas hipóteses, as operações de pagamento fraudulentas são operações mais do que autorizadas pelo titular do instrumento de pagamento: são realizadas por ele, devidamente autenticado, e através do seu dispositivo móvel, ainda que sem o esclarecimento que seria necessário para rejeitar a operação. Estas operações fraudulentas não são abrangidas pelo disposto no RSP2 quanto a operações não autorizadas porque são operações *autorizadas* pelo utilizador do serviço. A fraude, nestas hipóteses, tem na sua base a iliteracia informática — senão iliteracia *tout court* — do utilizador, agravada pela pressão da "engenharia social" de que é vítima, e estará sujeita à aplicação das regras gerais do direito civil, nomeadamente do erro-vício, dolo, ou situação de necessidade. Só não seria assim se o erro do utilizador fosse justificado pelas deficientes instruções fornecidas pelo prestador do serviço ou mesmo por um modo de funcionamento enganoso da aplicação.

6 Ónus da prova

A estas disposições sobre a imputação dos prejuízos provocados por operações de pagamento contestadas pelo utilizador do serviço acresce o disposto em matéria de prova, com a lei a manter sobre o prestador de serviços de pagamento o ónus da prova "*de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento*". Esclarece-se ainda que "*a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento (...) não é necessariamente suficiente, por si só, para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta, ou que não cumpriu, com dolo ou negligência grosseira, uma ou mais obrigações previstas no artigo 110.º*"[53]. Um aspecto importante introduzido no RSP 2, tal como decorre da directiva transposta, é a imposição ao prestador de serviços de pagamento, nos casos de operações contestadas pelo seu cliente, do ónus da prova da "*existência de fraude, de dolo ou de negligência grosseira da parte do utilizador de serviços de pagamento*", com vista a imputar-lhe os prejuízos causados pelas mesmas operações, nos termos explanados, ainda que, literalmente, o texto da lei prescreva

[53] Cfr. os n.ºs 1 e 3 do artigo 113.º do RSP 2.

que o prestador de serviços de pagamento "deve apresentar elementos que demonstrem" os graus de culpa indicados, e não utilize a expressão "ónus da prova"[54].

7 Reflexões conclusivas

A diversificação da oferta de instrumentos que permitem levar a cabo operações de pagamento electrónicas veio exigir uma rápida actualização tecnológica por parte dos prestadores de serviços de pagamento, impulsionada pela exigência de um reforço de segurança na autenticação dos utilizadores, com vista à diminuição dos riscos de operações fraudulentas. Esta autenticação reforçada dos utilizadores de instrumentos de pagamento não acautela, no entanto, a vulnerabilidade e a desactualização dos *softwares* utilizados em dispositivos móveis, a insegurança das *passwords* escolhidas pelo utilizador e a sua gravação nos dispositivos utilizados, a utilização de redes públicas para aceder a contas e para a realização de pagamentos e a imprudência do comportamento *online* de alguns utilizadores de serviços de pagamento móveis.

Por outro lado, o incremento da segurança técnica dos serviços de pagamento leva a que a montagem de novos esquemas fraudulentos incida sobre aquele que se apresenta como o "elo mais fraco" da cadeia de pagamentos: o utilizador. Assim, muitas das operações fraudulentas que são hoje levadas a cabo não têm na sua base sofisticados ataques informáticos que exponham as vulnerabilidades dos sistemas utilizados, mas sim técnicas de "engenharia social" que exploram a confiança natural dos utilizadores em terceiros ou que combinam a exploração dessa confiança com intromissões cibercriminosas.

A configuração variada dos esquemas fraudulentos levados a cabo para desencadear operações de pagamento não autorizadas exige dos prestadores de serviços uma acção pedagógica face aos seus clientes, sobretudo quando estes são consumidores[55], através de campanhas de sensibilização e de esclarecimento quanto a potenciais fraudes, ao mesmo tempo que lhes impõe uma monitorização constante relativamente às operações de pagamento efectuadas. A DSP de 2015 e o Regulamento Delegado (UE) 2018/389 que a complementa apontam já neste sentido. A DSP2 faz recair sobre o prestador do serviço um dever de gestão dos riscos operacionais e de segurança, incluindo "*medidas de mitigação e mecanismos de controlo adequados para gerir os riscos operacionais e de segurança, relacionados com os serviços de pagamento por si prestados*", e a criação e manutenção de "*procedimentos eficazes de gestão de incidentes, inclusive para a deteção e classificação de incidentes operacionais e de segurança de carácter severo*"[56]. E o Regulamento Delegado (UE) 2018/389, veio, por sua vez, estipular que os prestadores de serviços de pagamento devem dispor de mecanismos de controlo das operações que lhes permitam detectar operações de pagamento fraudulentas ou não autorizadas[57].

[54] Cfr. o n.º 4 do artigo 113.º do RSP 2. A importância desta regra é salientada por Reinhard Steennot, "Reduced payer's liability for unauthorized payment transactions...", cit., pp. 962-963, que afirma que, nestes casos, não será suficiente uma presunção de culpa baseada na simples utilização do instrumento de pagamento e das suas credenciais de segurança, exigindo-se outros meios de prova adicionais.

[55] No sentido de serem necessários esforços de educação do consumidor para a introdução de novos serviços de pagamento, v. também Maximilian Yang, "Card Payments and Consumer Protection in Germany", *in Anglo-German Law Journal*, 2, 2016, p. 26.

[56] Cfr. o artigo 95.º, n.º 1, da DSP 2, e o artigo 70.º, n.ºs 1 e 2, do RSP 2.

[57] Cfr., desde logo, o artigo 2.º, n.º 1, do Regulamento Delegado (UE) 2018/389. A DSP 1 permitia já ao prestador de serviços de pagamento incluir no

A antecipação e a prevenção de operações fraudulentas, ainda que seja um desígnio ambicioso, deverá ser o principal objectivo dos prestadores de serviços de pagamento, de modo a aumentar a confiança dos seus clientes, em especial dos consumidores, e a incentivar a utilização de novos instrumentos de pagamento.

contrato-quadro de utilização de um instrumento de pagamento a possibilidade de bloquear esse instrumento com base em razões objectivas de segurança ou de suspeita de fraude, possibilidade que se manteve na DSP 2, nos artigos 52.º, n.º 5, alínea *c)*, e 68.º, n.º 2.

Referências:

Banco de Portugal, *Relatório dos Sistemas de Pagamentos — 2020*, Lisboa, 2021, *in* https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/rsp2020.pdf (29.11.2023)

Banco de Portugal, *Relatório dos Sistemas de Pagamentos — 2019*, Lisboa, 2020, *in* https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/rsp2019_0.pdf (29.11.2023)

Barbosa, M. M., (2017) "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*), n.º 1, pp. 622-682, 2017-11-22, https://www.revistadedireitocomercial.com, (29.11.2023)

Correia, F. M., (2018) "Uma revolução permanente? A DSP 2 e o novo direito dos serviços de pagamento", *in III Congresso de Direito Bancário*, L. Miguel Pestana de Vasconcelos (coord.), Coimbra, Livraria Almedina, pp. 385-404

Donnelly, M., (2016) "Payments in the digital market: Evaluating the contribution of Payment Services Directive II", *in Computer Law & Security Review*, n.º 32, pp. 827-839

Duarte, P. A. P. (2021) "Os serviços de iniciação de pagamento no novo RSP", *in RED — Revista Electrónica de Direito*, vol. 25, n.º 2, Junho, pp. 37-83, *in* https://cij.up.pt//client/files/0000000001/3-patricia-duarte_1737.pdf, (29.11.2023)

EBA, *Single Rulebook Q&A*, Topic "Strong customer authentication and common and secure communication (incl. access)", question 2018_4042, *in* https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4042 (29.11.2023)

European Payments Council, *2019 Payment Threats and Fraud Trends Report*, EPC302-19/Version 1.0/Date issued: 9 December 2019, *in* https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2019-12/EPC302-19%20v1.0%202019%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf (29.11.2023)

Guerra, P., (2016) "A realização de operações de pagamento não autorizadas e a tutela do utilizador de serviços de pagamento em face do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica", *in RED — Revista Electrónica de Direito*, n.º 2, Junho, disponível em https://cij.up.pt//client/files/0000000001/2_648.pdf, (3.10.2023)

Guimarães, M. R., (2021) "Pagamentos electrónicos não autorizados e fraudulentos", *in Cibercriminalidade: novos desafios, ofensas e soluções*, Inês Sousa Guedes e Marcus Alan de Melo Gomes (eds.), Lisboa, Pactor – Edições de Ciências Sociais, Forenses e da Educação, pp. 227-240

Guimarães, M. R., (2021) "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, pp. 141-166

Guimarães, M. R., (2018) "O *phishing* de dados bancários e o *pharming* de contas. Análise jurisprudencial", *in III Congresso de Direito Bancário*, L. Miguel Pestana de Vasconcelos (coord.), Coimbra, Livraria Almedina, pp. 405-432

Guimarães, M. R., (2015) "(Ainda) a responsabilidade pelo uso indevido de instrumentos de pagamento electrónicos em operações presenciais e à distância, Análise do regime introduzido pelo Anexo I do Decreto-Lei n.º 317/2009, de 30 de Outubro (RSP), e das alterações que se perspectivam face à Proposta de Directiva do Parlamento Europeu e do Conselho, de 24 de Julho

de 2013", *in I Congresso de Direito Bancário*, L. Miguel Pestana de Vasconcelos (coord.), Coimbra, Livraria Almedina, pp. 115-144

Guimarães, M. R., (2013) "A fraude no comércio electrónico: o problema da repartição do risco por pagamentos fraudulentos", *in Infracções Económicas e Financeiras: Estudos de Criminologia e de Direito,* José Neves Cruz, Carla Cardoso, André Lamas Leite, Rita Faria (coords.), Coimbra, FDUP/Coimbra Editora, pp. 581-597

Guimarães, M. R., (2011) *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos*, Coimbra, Wolters Kluwer/Coimbra Editora

Guimarães, M.R., (1999) *As transferências electrónicas de fundos e os cartões de débito. Alguns problemas jurídicos relacionados com as operações de levantamento de numerário e de pagamento por meios electrónicos*, Coimbra, Livraria Almedina

Guimarães, M. R. / Steennot, R., (2022) "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, pp. 29-72

Lima, R. S. R., (2016) "A responsabilidade pela utilização abusiva *on-line* de instrumentos de pagamento eletrónico na jurisprudência portuguesa", *in RED — Revista Electrónica de Direito*, n.º 3, Outubro, *in* https://cij.up.pt//client/files/0000000001/3_658.pdf, (29.11.2023)

Pacheco J.M.N., (2016) "La nueva directiva 2015/2366 de servicios de pago en el mercado interior", *in Revista CESCO de Derecho de Consumo*, n.º 16, pp. 139-143, *in* https://revista.uclm.es/index.php/cesco, (29.11.2023)

Steennot, R., (2018) "Reduced payer's liability for unauthorized payment transactions under second Payment Services Directive (PSD2)", *in Computer Law & Security Review*, n.º 34, pp. 954-964

Steennot, R., (2021) "Liability for unauthorized payment transactions: the transposition of PSD2 in Belgium", *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, pp. 167-188

UK Finance, *Fraud - The Facts 2021, The definitive overview of payment industry fraud*, 2021, *in* https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf, (29.11.2023)

Woltersa, P.T.J. / Jacobs, B.P.F., (2019) "The security of access to accounts under the PSD2", *in Computer Law & Security Review*, n.º 35, pp. 29-41

Yang, M., (2016) "Card Payments and Consumer Protection in Germany", *in Anglo-German Law Journal*, n.º 2, pp. 6-38

2 *Suptech* e *Regtech* no contexto da atividade de regulação e supervisão

Luma Almeida e Joana Gama Gomes[58]

Abstract

The banking and financial sector has undergone several changes arising from the digital transformation and quite driven by the impact of COVID-19. The new paradigm of the financial services provision and the advent of the FinTech phenomenon have made clear the need to review the regulatory and supervisory metodologies. Institutions sought out processes that would facilitate regulatory compliance, given the high compliance costs they face, and, thus, supervisors saw the need and an opportunity to also take advantage of technology for supervisory purposes. In this path, the phenomena known as Regtech and Suptech emerged. The concepts, regulatory framework, benefits and challenges thereof will be explored throughout this study.

Glossário

Advanced visualization*:* Análise de dados com maior clareza, permitindo a absorção e compreensão rápida dos dados apresentados.[59]

Big data*:* Recolha, armazenamento, análise e aplicação de um grande volume e variedade de dados. Caracteriza-se frequentemente pelo aumento do volume, velocidade e variedade (os três Vs) de dados produzidos e refere-se tipicamente (mas não está limitado) a dados da Internet.[60]

Cloud computing*:* Utilização de uma rede online ("nuvem") de modo a aumentar a escala e a flexibilidade da capacidade informática. A computação em nuvem tornou possível a análise de conjuntos de dados muito grandes (grandes dados), e uma série de aplicações *fintech* específicas.[61]

Data analytics*:* Capacidade de analisar dados de forma mais rápida, eficiente, robusta e complexa do que utilizando técnicas de análise convencionais.[62]

[58] Departamento de Serviços Jurídicos do Banco de Portugal.

[59] Simone di Castri et al. — The Suptech Generations — FSI Insights on policy implementation No 19. 2019, página 5 (disponível em The suptech generations (bis.org).

[60] EBA Report On Big Data And Advanced Analytics January 2020, página 12 (disponível em Final Report on Big Data and Advanced Analytics.pdf (europa.eu)).

[61] Rodrigo Coelho et al. — Suptech applications for anti-money laundering — FSI Insights on policy implementation No 18 2019, página 18 (disponível em Suptech applications for anti-money laundering (bis.org)).

[62] Toronto Centre — Using Suptech to improve supervision: Essay Winners 2021. 2021, página 5 (disponível em Using_SupTech_to_Improve_Supervision.pdf (torontocentre.org)).

Fintech: Inovação tecnológica em serviços financeiros que poderá resultar em novos modelos de negócio, aplicações, processos ou produtos com um efeito material associado na prestação de serviços financeiros.[63]

Inteligência artificial (IA): Capacidade de uma máquina para apresentar capacidades semelhantes às humanas, como o raciocínio, a aprendizagem, o planeamento e a criatividade[64] [65]. Divide-se em três categorias: inteligência artificial fraca (conhecida como *Artificial Narrow Intelligence* (ANI)) — criada para se focar numa determinada área, com um objetivo específico; inteligência artificial média (conhecida como *Artificial General Intelligence* (AGI)) — que possui características como capacidade de raciocínio, compreensão de conceitos complexos e resolução de problemas; e inteligência artificial forte (conhecida como *Artificial Super Intelligence* (ASI)), cujas competências igualam ou superam as capacidades humanas e que ainda não existe.[66]

Machine-learning: Utilização e desenvolvimento de algoritmos e modelos estatísticos capazes de aprender com os dados e adaptar o seu desempenho sem serem explicitamente programados para o fazer.[67]

Natural language processing: Programação de computadores e algoritmos para analisar, processar e compreender a linguagem humana.[68]

Speech recognition: Processamento da fala humana num formato escrito.[69]

Sistema "push and pull": Entrega de dados pré-definidos da entidade regulada ao regulador ou supervisor, permitindo que esta autoridade obtenha dados da entidade regulada, conforme necessário.[70]

Tecnologia de registo distribuído: tecnologia que permite o funcionamento e a utilização de registos distribuídos, ou seja, de repositórios de informações que mantêm registos das transações e que são partilhados através de um conjunto de nós da rede DLT (dispositivos ou processos), encontrando-se sincronizados entre estes através de um mecanismo de consenso.[71]

Text mining: Processo de transformação de texto não estruturado num formato estruturado para identificar padrões significativos e novas perceções.[72]

[63] FSB — The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions — Market developments and financial stability implications. 2022, página 67 (disponível em The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions: Market developments and financial stability implications (fsb.org)).

[64] O que é a inteligência artificial e como funciona? | Atualidade | Parlamento Europeu (europa.eu)

[65] Note-se, no entanto, que ainda não existe uma definição consensualizada. A proposta de Regulamento de IA prevê uma definição bastante abrangente de sistema de inteligência artificial no seu artigo 3.º (1) por remissão para o anexo I do mesmo.

[66] Sónia Moreira, — "*IA e Robótica: A caminho da Personalidade Jurídica?*"*2022_IA-E-ROBOTICA.pdf (uminho.pt) (página 538).

[67] General Secretariat of the Council of the European Union — ChatGPT in the Public Sector — overhyped or overlooked?. 2023, página 19 (disponível em art-paper-chatgpt-in-the-public-sector-overhyped-or-overlooked-24-april-2023_ext.pdf (europa.eu)).

[68] FSB — The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions, página 67.

[69] What is Speech Recognition? | IBM.

[70] OCDE — 5. The use of SupTech to enhance market supervision and integrity *in* OECD Business and Finance Outlook 2021: AI in Business and Finance, página 134 (disponível em https://www.oecd-ilibrary.org/sites/d478df4c-en/index.html?itemId=/content/component/d478df4c-en).

[71] Artigo 2.º, n.º 1 do Regulamento (UE) 2022/858 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo a um regime-piloto para as infraestruturas de mercado baseadas na tecnologia de registo distribuído e que altera os Regulamentos (UE) n.º 600/2014 e (UE) n.º 909/2014 e a Diretiva 2014/65/UE.

[72] What is Text Mining? | IBM.

1 Introdução

1.1 Inovação tecnológica — diagnóstico e tendências

A transformação digital do setor bancário e financeiro da União Europeia, acelerada pela necessidade de resposta à pandemia da COVID-19, trouxe uma mudança profunda para o setor. Alterou o paradigma na prestação de serviços financeiros, que conta, agora, com modelos de negócio mais inovadores (assentes numa estrutura interna menos pesada e num relacionamento mais digital com os clientes), globalizados, para consumidores cada vez mais exigentes e *tech savvy*, abrindo portas a novos intervenientes de mercado.

A digitalização do setor e o aparecimento de novos *players* e de novas tecnologias obrigaram a banca tradicional a rever a sua proposta de valor, para atender a clientes que buscam soluções mais imediatas, personalizadas, flexíveis e disponíveis a qualquer momento e em qualquer lugar. Motivados pela pressão da aceleração tecnológica e digital, os atores do mercado tentam ir ao encontro das expectativas dos clientes e acompanhar as tendências globais.

A rápida disseminação de modelos de negócio com estruturas mais especializadas e de menor dimensão, nas quais a tecnologia assume um papel preponderante, com menores custos regulatórios e estruturas mais ágeis, ameaça a prestação de serviços como tradicionalmente a conhecíamos e obriga à revisão dos modelos de negócio pela banca tradicional.

O acima referido, aliado ao advento das *Fintech*[73], trouxe, na verdade, uma transformação que vai além das próprias instituições, obrigando, também, à revisão dos modelos de regulação e supervisão por parte das autoridades competentes. Com efeito, o desafio nasce no seio da indústria, mas reflete-se também nas autoridades, que procuram adaptar-se rapidamente às alterações trazidas pela digitalização do setor financeiro e redefinem estratégias para fazer face a esta evolução e acompanhá-la, revendo a forma como interagem com as instituições e a sua própria organização interna — dando, assim, lugar aos fenómenos que conhecemos como *Regtech* e *Suptech*.

Estes fenómenos não estão apenas dependentes da evolução dos sistemas tecnológicos. Na verdade, a relação entre entidades financeiras e autoridades, bidirecional, implica que o desenvolvimento e implementação de ferramentas *Regtech* e *Suptech* deverá ser oportunamente aceite pelas duas.[74]

Assim, por um lado, as aplicações tecnológicas a serem utilizadas pelas instituições têm de ser compatíveis com o enquadramento regulatório e com as práticas do supervisor, e, por outro, para que os avanços tecnológicos aplicados à atividade supervisiva das autoridades sejam efetivos, as instituições têm de estar preparadas para responder ao desafio das autoridades. Pelo que a articulação, a cooperação e a confiança entre instituições e autoridades revela-se, cada vez mais, essencial.

[73] Ou seja, "(...) à utilização de novas tecnologias no desenvolvimento e evolução dos serviços e produtos financeiros" (João Freire de Andrade; Margarida Mendes Maia — Fomentar a *Regtech*: o futuro da regulação financeira *in* António Menezes Cordeiro; Ana Perestrelo de Oliveira; Diogo Pereira Duarte — *Fintech* Novos estudos sobre tecnologia financeira. Coimbra: Almedina, 2019.

[74] Conforme destacado pela Professora Ana Paula Serra, "a velocidade e o alcance da transformação digital das funções de cumprimento e reporte regulatório e de conformidade das instituições financeiras está limitada pelo nível de transformação digital e de aceitação pelas autoridades" (SERRA, Ana Paula et al. — *Regtech* e *Suptech*. Infor Banca, *Revista do Instituto de Formação Bancária*, junho 2022, página 20 (disponível em InforBanca-125-JUN2022.pdf (ifb.pt)).

A inovação tecnológica tem contribuído significativamente para uma melhoria das ferramentas de supervisão e gestão de risco. É, portanto, um catalisador de eficiência e de outras múltiplas vantagens, comportando, porém, alguns desafios. Neste sentido, o principal contributo deste estudo assenta, sobretudo, na análise dos fenómenos de *Regtech* e *Suptech*, que adiante abordaremos, respetivo enquadramento normativo e principais benefícios e desafios, sobretudo de cariz jurídico.

1.2 Experiências das autoridades de regulação e supervisão

A inovação tecnológica e a digitalização tornaram-se prioridades estratégicas das autoridades, quer europeias, estando vertidas nas prioridades do Mecanismo Único de Supervisão (MUS) e nos trabalhos da Autoridade Bancária Europeia (EBA), do Banco Central Europeu (BCE) e da Comissão Europeia, quer nacionais, figurando, inclusivamente, no Plano Estratégico 2021-2025 do Banco de Portugal.

No plano da União Europeia (UE), no que se refere à Comissão Europeia destacam-se como pioneiras (i) a Estratégia para o Mercado Único Digital[75], que visa cumprir, entre outras prioridades, a criação do Mercado Único Digital (MUD), e (ii) a Estratégia em matéria de Financiamento Digital para a União Europeia[76].

Neste contexto, procura-se viabilizar uma transformação digital que garanta o respeito pelos valores da UE, proteja os direitos fundamentais e a segurança dos cidadãos e reforce a soberania digital da Europa. Os principais domínios de intervenção da estratégia digital da UE são os seguintes: (i) década digital — tendo sido criado um programa estratégico intitulado "Guião para a Década Digital", que define metas e marcos digitais a alcançar até 2030, (ii) declaração europeia sobre os direitos e princípios digitais, (iii) serviços digitais, (iv) economia dos dados, (v) tributação da economia digital, (vi) inteligência artificial, (vii) conectividade, (viii) cibersegurança, (ix) identidade digital europeia (e-ID) e (x) digitalização da justiça[77].

No plano internacional, o *Bank of International Settlements* (BIS), em particular através do *Innovation Hub*, tem-se debruçado sobre esta área, através do desenvolvimento de soluções *Suptech* e do acompanhamento das inovações em matéria de *Regtech* através de uma interação público-privada[78]. Destaca-se, em particular, o *Project Ellipse*[79], um projeto piloto que visa explorar a forma como a supervisão se poderá tornar mais *insight-based* e *data-driven*, utilizando uma plataforma integrada de dados regulamentares e analíticos. Este protótipo permite que as autoridades testem nos seus próprios ambientes e poderá ajudá-las a explorar novas soluções para o cumprimento da sua atividade. Configura, assim, uma oportunidade para as autoridades considerarem, explorarem e colaborarem em soluções comuns.

O potencial impacto transformador decorrente da utilização destas ferramentas de *Regtech* e *Suptech* levou a que, conforme notámos, a maioria das autoridades competentes na União Europeia tenha já desenvolvido, ou esteja em vias de desenvolver, estratégias e ferramentas de

[75] Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre a revisão intercalar relativa à aplicação da Estratégia para o Mercado Único Digital, de 10 de maio de 2017 (COM(2017) 228 final).

[76] 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 UE, de 24 de setembro de 2020 (COM(2020) 591 final).

[77] https://www.consilium.europa.eu/pt/policies/a-digital-future-for-europe

[78] BIS Innovation Hub work on suptech and regtech (disponível em BIS Innovation Hub work on Suptech and Regtech).

[79] Project Ellipse: an integrated regulatory data and analytics platform. BIS Innovation Hub, 2022 (disponível em https://www.bis.org/publ/othp48.pdf).

Suptech. Conforme nota o Administrador Hélder Rosalino "Estas inovações representam uma evolução crescente no papel desempenhado pela tecnologia na otimização dos processos internos e regulatórios, destacando o compromisso dos bancos centrais em alavancar tecnologias emergentes para fortalecer a eficiência e tempestividade da sua atuação."[80] De acordo com um estudo realizado pela EBA, as autoridades competentes indicaram 553 ferramentas de *Suptech*, das quais 216 estão já implementadas (39%), 163 estão em fase piloto (29%) e 160 em fase de ideia (29%).[81] O referido estudo concluiu, ainda, que as ferramentas de *Suptech* são, atualmente, mais utilizadas para fins macro-prudenciais, de proteção do consumidor/análise de conduta de mercado e relacionados com prevenção do branqueamento de capitais e do financiamento do terrorismo. Os principais desafios encontrados pelas autoridades dizem respeito aos recursos (insuficiência de recursos humanos e de aptidão/competência técnica) e a questões técnicas (decorrentes da alteração dos sistemas informáticos) e de governo (desafios quanto à complexidade e gestão destas soluções). Quanto às tecnologias maioritariamente utilizadas, destacam-se a análise de dados (*data analytics*) e *big data*, *text mining* e processamento de linguagem natural (*natural language processing*), interfaces de programação de aplicativos (a*pplication programming interface — API*), inteligência artificial e *machine-learning* (27%), e visualização avançada (*advanced visualization*)[82].

2 *Regtech* e *Suptech*

A transformação digital tem vindo a produzir impactos nas instituições e autoridades, que não ficam indiferentes, nem inertes, face a este novo "maremoto tecnológico". O célere desenvolvimento tecnológico no setor bancário e financeiro trouxe desafios à regulação nos moldes tradicionais. As instituições e os novos intervenientes buscam um enquadramento regulatório que não aniquile o seu propósito e respetivo crescimento e as autoridades sentem a necessidade de cooperar com as instituições e com os novos *players* na determinação de tendências de atividade e na definição de limites[83] — permitindo, assim, a evolução do setor com as salvaguardas necessárias, nomeadamente, à garantia da estabilidade financeira e da proteção do consumidor — uma vez que a evolução do regulado sem a correspondente evolução do regulador poderá comportar riscos e trazer ameaças adicionais para o setor[84].

Se, por um lado, a regulação desenvolvida na sequência da crise financeira global de 2008 aumentou os requisitos e reportes a cumprir por parte das instituições, reforçando a importância da eficiência e efetividade no cumprimento da regulação, por outro lado, tornou evidente a necessidade de uma monitorização mais eficiente e em tempo-real, que permita uma supervisão mais preditiva e que beneficie, respeitados os limites, do aumento de dados disponíveis.

O conceito de *Regtech*, que decorre da junção dos termos "*regulatory*" e "*technology*", corresponde à utilização da tecnologia para fins de cumprimento de normas legais e regulamentares, bem

[80] https://www.eba.europa.eu/assets/2023-Annual-Report/en/index.html. Artigo de opinião do Administrador Hélder Rosalino no livro "88 Vozes sobre Inteligência Artificial" — A Inteligência Artificial ao serviço dos bancos centrais | Banco de Portugal (bportugal.pt)

[81] https://www.eba.europa.eu/assets/2023-Annual-Report/en/index.html

[82] //http://www.eba.europa.eu/assets/2023-Annual-Report/en/index.html

[83] João Freire de Andrade; Margarida Mendes Maia — Fomentar a Regtech: o futuro da regulação financeira, *op. cit.*, página 10.

[84] Stefan Zeranski; Ibrahim E Sancak. — *Digitalization of Financial Supervision with Supervisory Technology (Suptech)* in *Journal of International Banking Law & Regulation*, 10 agosto 2022, página 4 — "*There must be at least parallel developments between FinTech and Suptech to protect the financial system and financial consumers against FinTech related risks and threats. A FinTech dominant financial sector without Suptech signals huge risks for an economy*".

como de outros instrumentos regulatórios. Visa, sobretudo, através da utilização da tecnologia, melhorar os processos internos, mediante a utilização de soluções tecnológicas concebidas para o cumprimento de requisitos regulatórios, de conformidade e de reporte.

As ferramentas de *Regtech* são utilizadas, maioritariamente, para fins de[85]:

- Prevenção do branqueamento de capitais e combate ao financiamento do terrorismo;
- Reporte e cumprimento regulatório (*compliance*);
- Gestão de identidade e controlo (processos de "*Know Your Customer*" (KYC));
- Gestão de risco;
- Monitorização de operações;
- Transações em mercado financeiro.

As tecnologias utilizadas concentram-se na utilização de protocolos de transferência de dados, serviços de computação em nuvem (*cloud*) e técnicas de inteligência artificial.

O recurso a estas ferramentas de *Regtech* traz diversos benefícios, que incluem: (i) o aumento da eficiência e efetividade, (ii) a melhoria da inteligibilidade e interoperabilidade dos dados (ao reduzir a sua complexidade e transformá-los em indicadores acessíveis), (iii) a redução do erro humano, (iv) o aumento da capacidade de monitorização e de identificar e analisar riscos de forma mais rápida e eficiente, (v) o cumprimento dos deveres regulatórios e o acompanhamento das alterações de forma mais fácil e célere, (vi) a automatização de tarefas de rotina, que permite que os colaboradores se foquem em tarefas de valor-acrescentado e gera ganhos com poupança de custos com recursos humanos que estavam afetos a essas tarefas, e (vii) a prestação de informação e análise de riscos em tempo-real e com uma análise mais preditiva.

Contudo, traz também diversos desafios, entre os quais: (i) a necessidade de assegurar a disponibilidade operacional da entidade (incluindo dispor de recursos especializados); (ii) alterações ao *compliance* regulatório existente; (iii) a necessidade de prevenir falhas no acompanhamento das novidades regulatórias; (iv) a necessidade de mitigação dos riscos operacionais derivados da utilização da tecnologia (incluindo ciber-riscos e riscos de *outsourcing*) e os riscos decorrentes da ausência de uma posição uniforme por parte dos reguladores; (v) a gestão dos custos elevados e o tempo de desenvolvimento das interfaces de programação de aplicação (*Application Programming Interface* — API) — sendo certo que estes custos são maiores para os primeiros criadores; (vi) a gestão do impacto nos trabalhadores que estão afetos a tarefas automatizáveis — desafios com reconversão ou custos financeiros, sociais e reputacionais com a sua saída; e (vii) a criação de risco sistémico por alguns fornecedores de *Regtech* (ex.: fornecedores de sistemas *cloud*).

Por sua vez, o conceito de *Suptech* (por vezes também chamada "*Regtech para reguladores*"[86]) advém da combinação dos termos "*supervisory*" e "*technology*" e corresponde à adoção de soluções tecnológicas por parte das autoridades no exercício da atividade de supervisão, por forma a torná-la mais ágil e preditiva. Num contexto de acelerada inovação tecnológica no setor financeiro, a utilização de ferramentas de *Suptech* torna possível a extração e o tratamento massivo de dados e informações com o objetivo de melhorar a supervisão, intensificando uma abordagem baseada em dados e no risco e em regras e princípios. Ora, conforme destaca o

[85] International Association of Insurance Supervisors — *Regtech and Suptech: Implications for Supervision*, março 2019, página 3.
[86] João Freire de Andrade; Margarida Mendes Maia — Fomentar a Regtech: o futuro da regulação financeira, *op. cit.*

Administrador do Banco de Portugal, Hélder Rosalino, no livro *88 Vozes sobre Inteligência Artificial* — A Inteligência Artificial ao serviço dos bancos centrais "*Combinada com tecnologias inovadoras e disruptivas, como a aprendizagem automática ou o processamento de linguagem natural, a utilização de grandes volumes de dados nos bancos centrais oferece, sem dúvida, novas oportunidades para melhor compreender a economia e o sistema financeiro e, nessa linha, para apoiar a formulação de políticas e produzir conhecimento*."[87]

Mais de metade das autoridades competentes (de supervisão bancária) na União Europeia já têm ou estão em vias de desenvolver uma estratégia ou plano de implementação de ferramentas de *Suptech*.

As ferramentas de *Suptech* são utilizadas pelas autoridades de supervisão e de resolução, sobretudo, para os seguintes fins:

- Supervisão micro-prudencial (para fins de interação com a indústria, reportes regulares, análise de dados, *fit and proper*, análise de riscos de crédito, das tecnologias de informação e comunicação — e outros riscos operacionais — e de liquidez, *stress tests*);
- Processamento e análise de dados;
- Prevenção do branqueamento de capitais e combate ao financiamento do terrorismo (reporte, análise de dados e *risk scoring*);
- Monitorização das redes sociais e da *dark web*;
- Proteção dos consumidores e supervisão de conduta (análise de dados, tratamento e análise de reclamações, análise de riscos e supervisão de mercado);
- Supervisão macro-prudencial (identificação de riscos emergentes);
- Proteção de depósitos (verificação de ficheiros CSV (valores separados por vírgulas), processo automatizado de criação de *Payment Instruction Files*, registo e reconciliação de montantes pagos e cálculo de montantes a ser reembolsados);
- Resolução (reportes, recolha de dados *ad hoc*, cálculos de contribuições para o fundo de resolução).

Estas ferramentas de *Suptech* trazem diversos benefícios, que incluem: (i) ganhos de eficiência e efetividade (análise mais célere e com melhor capacidade analítica global); (ii) identificação de *outliers* ; (iii) redução do erro humano; (iv) reforço da gestão de risco; (v) melhoria da experiência da supervisão, melhorando a supervisão em tempo-real e a automatização de processos (possibilitando uma supervisão mais preditiva e pró-ativa); (vi) melhoria da tomada de decisão baseada em factos e redução dos preconceitos cognitivos; e (vii) melhoria da capacidade de obtenção automática de informação significativa (capacidade de recolha massiva e célere de dados).

Contudo, a utilização destas ferramentas comporta também alguns riscos e desafios, dos quais se destacam:

[87] Artigo de opinião do Administrador Hélder Rosalino no livro *88 Vozes sobre Inteligência Artificial* — A Inteligência Artificial ao serviço dos bancos centrais | Banco de Portugal (bportugal.pt)

- os seguintes riscos: (i) fiabilidade/qualidade (incluindo, o enviesamento)[88] e a ausência de dados padronizados[89]; (ii) delegação excessiva[90]; (iii) risco jurídico, operacional (ciber-riscos, riscos operacionais e de "*gaming the system*"[91]) e reputacional; e (iv) confidencialidade (utilização de dados pessoais, acesso a segredos comerciais e a informação sensível); e
- os seguintes desafios: (v) atração e retenção de recursos humanos qualificados (com competências e habilitações adequadas)[92]; e (vi) em matéria de *governance* (complexidade de gestão dos projetos, dificuldades em fazer o *set-up* e adaptar os processos e procedimentos, falta de objetivos e metas claras).

As autoridades monitorizam os desenvolvimentos em matéria de *Suptech* acompanhando as tendências e o desenvolvimento tecnológico do setor, bem como os projetos implementados em outras organizações nacionais e internacionais, participando em grupos e fóruns de discussão destas matérias e partilhando experiências.

[88] "*In machine learning, the model's algorithm will only be as good as the data it trains on* (...) *This means biased data will result in biased decisions" — Artificial Intelligence and Machine Learning: Policy Paper*, *Internet Society*, Abril 2017 (disponível em Artificial Intelligence & Machine Learning: Policy Paper | Internet Society).

[89] Trata-se de um processo de conversão dos dados num formato padrão que pode ser lido, processado e analisado e que permite que diferentes sistemas partilhem e utilizem os dados de forma eficiente.

[90] Poderá existir uma tentação de "delegar" o exercício de funções ou competências nestas ferramentas, isto é, de que o exercício de determinadas funções por parte dos supervisores seja assegurado de forma exclusiva, ou quase, por tais instrumentos (p. ex. respostas a supervisionados ou a reclamações ou determinados atos integrados em procedimentos administrativos).

[91] "*One example is the risk of 'reward hacking' where the AI agent finds a way of doing something that might make it easier to reach the goal, but does not correspond with the designer's intent* [...] *There is also a risk that autonomous systems are exploited by malicious actors trying to manipulate the algorithm.*", *Artificial Intelligence and Machine Learning: Policy Paper*, *Internet Society*, Abril 2017 (disponível em Artificial Intelligence & Machine Learning: Policy Paper | Internet Society).

[92] "*Além disso, destacam-se os desafios associados à capacitação e reconversão da força de trabalho existente para se adequar a essas novas áreas de conhecimento, bem como à contratação de novos profissionais especializados em questões relacionadas com big data e inteligência artificial.*" em Artigo de opinião do Administrador Hélder Rosalino no livro "88 Vozes sobre Inteligência Artificial" — A Inteligência Artificial ao serviço dos bancos centrais

3 Enquadramento normativo da utilização de tecnologia financeira

3.1 No contexto da União Europeia

A. Legislação europeia

A União Europeia[93] deu o primeiro passo no âmbito do financiamento digital, em março de 2018, com a divulgação, pela Comissão Europeia, do "Plano de Ação para a Tecnologia Financeira: rumo a um setor financeiro europeu mais competitivo e inovador" (usualmente denominado "*FinTech Action plan*")[94]. Neste plano, a Comissão afirma, em particular, que "a tecnologia financeira (...)oferece oportunidades (...) em termos de conformidade e de supervisão regulamentares", podendo "facilitar, simplificar e automatizar os procedimentos de conformidade e de comunicação de informações e melhorar a supervisão"[95].

O Plano de Ação estabelece três áreas prioritárias para a ação da União — permitir aos modelos empresariais inovadores alcançar uma dimensão à escala da UE, apoiar a adoção da inovação tecnológica no setor financeiro e reforçar a segurança e a integridade do setor financeiro.

Este Plano determina, ainda, várias exigências que devem moldar a ação regulatória da União no domínio do *digital finance*. Entre outras, destacam-se, em particular, as decorrentes (i) do princípio da neutralidade tecnológica, (ii) do princípio da proporcionalidade e (iii) da integridade do mercado[96].

O princípio da neutralidade tecnológica constitui "um dos princípios orientadores das políticas da Comissão"[97] e dá resposta à liberdade dos indivíduos e organizações de escolherem a tecnologia mais apropriada e adequada às suas necessidades, exigindo que a regulação não favoreça nem discrimine a utilização de um determinado tipo de tecnologia.

Já o princípio da proporcionalidade, decorrente do artigo 5.º, n.º 4, do Tratado da União Europeia (TUE), determina que, na sua atuação, a UE deve adotar apenas as medidas que são adequadas e necessárias para concretizar os seus objetivos. Por essa razão, também no âmbito da regulação e supervisão, as autoridades competentes devem evitar impor às entidades supervisionadas custos de conformidade excessivos, que afetem a sua viabilidade ou que tornem mais difícil a inovação[98].

[93] Além da aprovação, pela União Europeia, de planos relacionados com a tecnologia financeira, destaca-se a aprovação, em 2018, de um plano coordenado para a IA (*Coordinated Plan on Artificial Intelligence*) que pretende acelerar os investimentos em tecnologias de IA para impulsionar uma recuperação económica e social resiliente; agir em conformidade com as estratégias e programas de IA e alinhar a política de IA para eliminar a fragmentação e enfrentar os desafios globais (*Coordinated Plan on Artificial Intelligence | Shaping Europe's digital future* (europa.eu)).

[94] Comunicação da Comissão "Plano de Ação para a Tecnologia Financeira: rumo a um setor financeiro europeu mais competitivo e inovador" (COM(2018) 109 final), de 8 de março de 2018.

[95] A Comissão ressalva, porém, que a utilização da tecnologia financeira traz, também, alguns desafios associados. Destaca, em particular, os casos em que as entidades reguladas [ou supervisionadas] recorrem a esta tecnologia por via da prestação de serviços externos, afirmando que estas "continuam a ser responsáveis pelo cumprimento das suas obrigações", não podendo "delegar a responsabilidade do cumprimento destes requisitos nos prestadores de serviços externos". Comunicação da Comissão "Plano de Ação para a Tecnologia Financeira: rumo a um setor financeiro europeu mais competitivo e inovador" (COM(2018) 109 final), de 8 de março de 2018.

[96] Estes princípios são, por exemplo, referenciados nos considerandos 9 e 10 do Regulamento (UE) 2022/858 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo a um regime-piloto para as infraestruturas de mercado baseadas na tecnologia de registo distribuído.

[97] Plano de Ação para a Tecnologia Financeira, ponto 2.1.

[98] Plano de Ação para a Tecnologia Financeira, pontos 1.1. e 1.3.

Por fim, a ação da União deverá sempre visar garantir a proteção da integridade e da credibilidade dos mercados. Desta forma, a regulação deverá promover um aumento da concorrência, melhorar a interoperabilidade e simplificar o intercâmbio de dados entre intervenientes do mercado e o seu acesso a estes[99].

Já em fevereiro de 2020, foi publicada, pela Comissão Europeia, a "Estratégia em matéria de Financiamento Digital para a UE" ("*Digital Finance Strategy for the EU*")[100]. A estratégia apresenta quatro prioridades para a transformação digital do setor financeiro da União:

a) combater a fragmentação do mercado único digital de serviços financeiros, de modo a facultar aos consumidores europeus o acesso aos serviços transfronteiras e ajudar as empresas financeiras europeias a incrementar as suas operações digitais ("primeira prioridade");

b) assegurar que o quadro regulamentar da UE facilita a inovação digital no interesse dos consumidores e da eficiência do mercado ("segunda prioridade");

c) criar um espaço europeu de dados financeiros para promover a inovação baseada em dados, assente na estratégia europeia para os dados, incluindo um melhor acesso aos dados e uma maior partilha de dados no setor financeiro ("terceira prioridade");

d) enfrentar os novos desafios e riscos associados à transformação digital ("quarta prioridade").

Em particular, quanto à terceira prioridade, a Comissão referiu que "Até 2024, a UE visará criar as condições necessárias para permitir a utilização de tecnologias inovadoras, incluindo *Regtech* e *Suptech*, para efeitos da comunicação de informações pelas entidades regulamentadas e de supervisão pelas autoridades competentes". Quanto a este ponto, a Comissão refere que pretende, igualmente, que "os elementos essenciais da regulamentação da UE possam ser objeto de processamento de linguagem natural, sejam legíveis e executáveis por máquinas e facilitem, de modo geral, a definição e aplicação dos requisitos em matéria de comunicação de informações".

Igualmente em fevereiro de 2020 foi aprovada a Estratégia Europeia para os Dados (também conhecida como "*European Data Strategy*")[101], que visa garantir o papel de liderança da UE numa sociedade impulsionada pelos dados. O objetivo da estratégia consiste na promoção de um mercado único dos dados, permitindo a sua circulação de forma fluída dentro da UE, o cumprimento das regras europeias, nomeadamente em matéria de privacidade, de proteção dos dados pessoais e de direito da concorrência, assim como a clareza das regras de acesso aos dados[102].

[99] Plano de Ação para a Tecnologia Financeira, ponto 1.2.

[100] 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 UE, de 24 de setembro de 2020 (COM(2020) 591 final).

[101] Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e a o Comité das Regiões sobre uma Estratégia Europeia para os Dados, de 19 de fevereiro de 2020 (COM(2020) 66 final).

[102] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_pt.

Para a concretização desta estratégia, foram propostos dois Regulamentos, complementares entre si: o Regulamento Europeu sobre a Governação de Dados, atualmente já aplicável[103], e o Regulamento dos Dados[104].

O primeiro visa aumentar a confiança na partilha de dados, reforçar os mecanismos para aumentar a disponibilidade de dados e superar os obstáculos técnicos à reutilização dos dados[105]. Verifica-se, também, a criação e o desenvolvimento de espaços comuns europeus de dados em domínios estratégicos, envolvendo intervenientes privados e públicos (*vide* considerando 2).

Por outro lado, a proposta do Regulamento dos Dados visa impulsionar a economia de dados da UE, alimentada pela Internet das Coisas (do inglês, *Internet of Things*), desbloqueando os dados industriais, otimizando a sua acessibilidade e utilização e promovendo um mercado europeu de computação em nuvem competitivo e fiável.

Têm, ainda, sido propostos e publicados vários outros atos jurídicos com vista à regulação da utilização da tecnologia financeira no espaço da União Europeia.

Em 2019, foram publicadas, pela Autoridade Bancária Europeia, as Orientações relativas à subcontratação (usualmente designada "*outsourcing*") ("EBA/GL/2019/02") e as Orientações relativas à gestão dos riscos associados às tecnologias de informação e comunicação (TIC) e à segurança ("EBA/GL/2019/04"). As primeiras visam estabelecer disposições de governo interno que as instituições de crédito, as instituições de pagamento e as instituições de moeda eletrónica devem implementar quando subcontratam funções, em particular no que se refere à subcontratação de funções essenciais e importantes[106]. As segundas especificam as medidas de gestão dos riscos que as instituições financeiras e os prestadores de serviços de pagamento devem adotar para gerir os seus riscos associados às TIC e à segurança, como os riscos operacionais, para todas as atividades prestadas[107].

Já em 2022, foram publicados dois Regulamentos essenciais no domínio dos mercados digitais — o Regulamento dos Serviços Digitais (RSD)[108] e o Regulamento dos Mercados Digitais (RMD)[109], que consagram um novo conjunto de regras com o objetivo de contribuir para o bom funcionamento do mercado interno dos serviços digitais, criando, ainda, mecanismos de supervisão pública das plataformas tecnológicas no espaço da UE.

Foi, igualmente, publicado, em 2022, o Regulamento relativo a um regime-piloto para as infraestruturas de mercado baseadas na tecnologia de registo distribuído (Regulamento DLT)[110],

[103] Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho, de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724.

[104] Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, de 13 de dezembro de 2023, relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização e que altera o Regulamento (EU) 2017/2394 e a Diretiva (UE) 2020/1828.

[105] Considerando 5 do Regulamento Europeu sobre a Governação de Dados.

[106] Orientações da EBA relativas à subcontratação, de 25 de fevereiro de 2019 (EBA/GL/2019/02) (disponível em EBA BS 2019 xxx (EBA Draft Guidelines on outsourcing arrangements).docx (europa.eu)), ponto 5.

[107] Orientações da EBA relativas à gestão dos riscos associados às TIC e à segurança, de 8 de novembro de 2019 (EBA/GL/2019/04) (disponível em EBA BS 2019 XXX (Final draft Guidelines on ICT and security risk management).docx (europa.eu)), ponto 6.

[108] Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE.

[109] Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho de 14 de setembro de 2022 relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828.

[110] Regulamento (UE) 2022/858 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo a um regime-piloto para as infraestruturas de mercado baseadas na tecnologia de registo distribuído e que altera os Regulamentos (UE) n.º 600/2014 e (UE) n.º 909/2014 e a Diretiva 2014/65/UE.

destinado a promover a adoção de uma tecnologia transformadora — a tecnologia de registo distribuído — no setor financeiro.

Em dezembro de 2022, foi publicado o Regulamento relativo à resiliência operacional digital do setor financeiro (DORA)[111], que estabelece requisitos uniformes para a segurança das redes e dos sistemas de informação das empresas e organizações que operam no setor financeiro, bem como para terceiros essenciais que lhes prestam serviços relacionados com as TIC.

Destaca-se, também, a publicação, em 2023, do Regulamento relativo aos mercados de criptoativos (MiCA)[112], que estabelece requisitos uniformes para a oferta pública e a admissão à negociação numa plataforma de negociação de criptoativos que não sejam criptofichas referenciadas a ativos nem criptofichas de moeda eletrónica, de criptofichas referenciadas a ativos e de criptofichas de moeda eletrónica, bem como requisitos aplicáveis aos prestadores de serviços de criptoativos (artigo 1.º, n.º 1).

Igualmente relevantes no âmbito da utilização da tecnologia na área financeira, são, ainda, a proposta de Regulamento que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento IA)[113] e a proposta de Diretiva relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial (Diretiva Responsabilidade IA)[114].

Estas duas últimas propostas preveem a sua aplicação às autoridades públicas (artigo 3.º, n.º 2, do Regulamento IA e artigo 2.º, n.º 3, da Diretiva Responsabilidade IA).

O Regulamento IA enquadra os sistemas de IA tendo em conta o risco gerado pela sua utilização, classificando-os em três tipos — risco inaceitável (artigo 5.º), risco elevado (artigo 6.º e ss.) e risco baixo ou mínimo.

Os sistemas de IA de risco inaceitável integram as designadas "práticas proibidas", que incluem todos os sistemas de IA cuja utilização seja considerada inaceitável por violar os valores da União — por exemplo, por violar os direitos fundamentais[115].

O segundo grupo integra os sistemas de IA que, não sendo de risco inaceitável, criam, ainda assim, um risco elevado para a saúde, a segurança ou os direitos fundamentais de pessoas singulares. Estes sistemas são autorizados a operar no mercado europeu, estando, porém, sujeitos ao cumprimento de determinados requisitos obrigatórios e a uma avaliação da conformidade *ex ante*.

[111] Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011.

[112] Regulamento (UE) 2023/1114 do Parlamento Europeu e do Conselho de 31 de maio de 2023 relativo aos mercados de criptoativos e que altera os Regulamentos (UE) n.o 1093/2010 e (UE) n.o 1095/2010 e as Diretivas 2013/36/UE e (UE) 2019/1937.

[113] Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial e altera determinados atos legislativos da União, de 21 de abril de 2021 (COM/2021/206 final) (disponível em resource.html (europa.eu). Em dezembro de 2023, o Parlamento Europeu e o Conselho da União Europeia chegaram a acordo sobre um texto comum com vista à adoção do Regulamento IA (disponível em https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai).

[114] Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial, de 28 de setembro de 2022 (COM(2022) 496 final) (disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52022PC0496).

[115] As proibições abrangem práticas com potencial significativo para manipular as pessoas por meio de técnicas subliminares que lhes passam despercebidas ou explorar as vulnerabilidades de grupos específicos para distorcer substancialmente o seu comportamento de uma forma que seja suscetível de causar danos psicológicos ou físicos a essa ou a outra pessoa. Outras práticas manipuladoras ou exploratórias que são possibilitadas pelos sistemas de IA podem, ainda, ser abrangidas pela legislação em matéria de proteção de dados, de defesa dos consumidores e de serviços digitais. A proposta proíbe, também, a classificação social assente na IA para uso geral por parte das autoridades públicas.

O anexo III da proposta de Regulamento enumera os sistemas de IA incluídos no conceito de "sistema de IA de risco elevado". Consideram-se particularmente relevantes para o tema deste estudo, nomeadamente, os sistemas de IA concebidos para:

- "serem utilizados para avaliar a capacidade de endividamento de pessoas singulares ou estabelecer a sua classificação de crédito, com exceção dos sistemas de IA colocados em serviço por fornecedores de pequena dimensão para utilização própria" (n.º 5.º, alínea b));
- "serem utilizados por autoridades policiais em avaliações individuais de riscos relativamente a pessoas singulares, a fim de determinar o risco de uma pessoa singular cometer infrações ou voltar a cometer infrações ou o risco para potenciais vítimas de infrações penais" (n.º 6.º, alínea a));
- "auxiliar uma autoridade judiciária na investigação e na interpretação de factos e do direito e na aplicação da lei a um conjunto específico de factos" (n.º 8.º, alínea a)).

Por fim, para os sistemas de risco baixo ou mínimo, o Regulamento IA estabelece um quadro para a criação de códigos de conduta, que visa incentivar os fornecedores destes sistemas de IA a aplicar voluntariamente os requisitos obrigatórios aplicáveis aos sistemas de IA de risco elevado. A classificação destes sistemas de IA gera obrigações para todos os agentes da cadeia (fornecedores, distribuidores, utilizadores), quer sejam autoridades públicas, quer entidades privadas.

Quanto à Diretiva Responsabilidade IA, esta propõe estabelecer requisitos uniformes para certos aspetos da responsabilidade civil extracontratual por danos causados pela utilização de sistemas de IA, visando uma harmonização mínima nesta matéria. As suas disposições serão aplicáveis a ações de indemnização de direito civil por danos causados por um sistema de IA, sempre que tais ações sejam intentadas ao abrigo de regimes de responsabilidade culposa extracontratual (que preveem a responsabilidade legal de indemnizar os danos causados intencionalmente ou por ação ou omissão negligente).

As normas introduzidas por este diploma visam, essencialmente, a possibilidade de imposição da disponibilização de elementos de prova (artigo 3.º) e o estabelecimento de uma presunção (ilidível) da existência de nexo de causalidade em caso de culpa (artigo 4.º).

Estas normas aplicam-se, tanto aos fornecedores, como aos utilizadores, de sistemas de IA (artigo 3.º, n.º 1). No quadro da Diretiva, considera-se "fornecedor" "uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que desenvolva um sistema de IA ou que tenha um sistema de IA desenvolvido com vista à sua colocação no mercado ou colocação em serviço sob o seu próprio nome ou marca, a título oneroso ou gratuito".

Já um "utilizador" será "uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que utilize, sob a sua autoridade, um sistema de IA, salvo se o sistema de IA for utilizado no âmbito de uma atividade pessoal de caráter não profissional".

As disposições da Diretiva aplicam-se, assim, tanto a entidades públicas, como privadas.

B. Princípios de Direito da União Europeia

Além das normas constantes dos diplomas acima descritos, é, igualmente, relevante e necessário, no âmbito da atividade das autoridades públicas aquando da utilização de ferramentas tecnológicas (e, em particular, nos processos que envolvam a tomada de decisões), que seja assegurado o respeito por princípios e garantias fundamentais traduzidos em

princípios de Direito da União[116], tais como a tutela jurisdicional efetiva (artigo 47.º da Carta dos Direitos Fundamentais da UE (CDFUE)), o princípio da boa administração (artigos 298.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e 41.º da CDFUE), o princípio da proporcionalidade (artigos 5.º do TUE, 3.º do TFUE e 52.º da CFDUE) e o princípio da igualdade (artigo 20.º da CDFUE).

Quanto a estas garantias, importa destacar, em particular, o direito a uma boa administração, regulado no artigo 41.º da CDFUE, que determina que todas as pessoas têm direito a que os seus assuntos sejam tratados pelas instituições, órgãos e organismos da União de forma imparcial, equitativa e num prazo razoável (n.º 1). Segundo o artigo 41.º, este direito compreende, nomeadamente, o direito de qualquer pessoa a ser ouvida antes de a seu respeito ser tomada qualquer medida individual que a afete desfavoravelmente (artigo 41.º, n.º 2, alínea a)), o direito de qualquer pessoa a ter acesso aos processos que se lhe refiram, no respeito pelos legítimos interesses da confidencialidade e do segredo profissional e comercial (artigo 41.º, n.º 2, alínea b)), e a obrigação, por parte da Administração, de fundamentar as suas decisões (artigo 41.º, n.º 2, alínea c)). Esta disposição prescreve, ademais, que todas as pessoas têm direito à reparação, por parte da União, dos danos causados pelas suas instituições ou pelos seus agentes no exercício das respetivas funções, de acordo com os princípios gerais comuns às legislações dos Estados-Membros (artigo 41.º, n.º 3).

As implicações do princípio da boa administração, no que diz respeito à atuação das autoridades públicas, foram, inicialmente, alvo de densificação pela jurisprudência do Tribunal de Justiça da União Europeia (TJUE) e, só mais tarde, consagradas na CDFUE.

Em particular, no âmbito dos processos administrativos que dizem respeito a avaliações técnicas complexas, o TJUE reconhece que as autoridades públicas devem dispor de um "determinado poder de apreciação" no exercício das suas funções[117]. No entanto, "nos casos em que as autoridades dispõem de um tal poder amplo de apreciação", o TJUE esclareceu que "o respeito das garantias atribuídas pela ordem jurídica comunitária nos processos administrativos assume uma importância ainda mais fundamental. De entre essas garantias, constam, nomeadamente, a obrigação para a instituição competente de examinar, com cuidado e imparcialidade, todos os elementos relevantes do caso em apreço, o direito do interessado a dar a conhecer o seu ponto de vista, bem como o direito a uma fundamentação suficiente da decisão. Só assim, é que o Tribunal pode verificar se os elementos de facto e de direito, de que depende o exercício do poder de apreciação, estão reunidos"[118].

Estas exigências configuram, assim, importantes contrapartidas face ao exercício de um poder discricionário por parte da instituição pública, o que implicará, consequentemente, por parte desta, o cumprimento de um elevado grau de diligência e de zelo, que o TJUE poderá, naturalmente, avaliar.

[116] Veja-se, neste sentido, que, na exposição de motivos do Regulamento IA, a própria Comissão Europeia defende a importância da preservação da liderança da UE no que concerne aos desenvolvimentos tecnológicos, salientando que a regulamentação de tais tecnologias permitirá a salvaguarda dos direitos e princípios fundamentais da União, protegendo, dessa forma, os cidadãos europeus. Além das preocupações enunciadas, a Comissão também apresenta outros objetivos específicos, como garantir a segurança jurídica para facilitar os investimentos e facilitar o desenvolvimento do mercado único.

[117] Acórdão do Tribunal de Justiça de 21 de novembro de 1991, *Hauptzollamt München-Mitte* c. *Technische Universität München*, processo C–269/90, ECLI:EU:C:1991:438, parágrafo 13. Este poder de apreciação é, também hoje, comummente designado como "poder discricionário".

[118] *Idem*, parágrafo 14.

Assim, ainda que o TJUE reconheça às autoridades públicas uma margem de apreciação relevante em decisões que implicam avaliações discricionárias e complexas, tal não significa que este Tribunal se abstenha de fiscalizar a interpretação que a autoridade pública fez dos elementos do caso concreto nem a razoabilidade das suas conclusões, face ao dever de diligência que sobre ela impende. O TJUE não substitui a sua própria avaliação pela análise da autoridade administrativa competente, no que se refere aos méritos da decisão em causa, embora exerça um controlo, que pode ser exigente e "apertado", da decisão da Administração, em face do dever de diligência aplicável. O TJUE deve, designadamente, não só verificar a exatidão material dos elementos de prova invocados, mas também fiscalizar se estes elementos constituem a totalidade dos dados pertinentes que devem ser tomados em consideração para apreciar uma situação complexa e se são suscetíveis de fundamentar as conclusões que deles se retiram.

Por fim, importa, igualmente, referir que, no âmbito da União Bancária, o Regulamento (UE) n.º 1024/2013 do Conselho de 15 de outubro de 2013, que confere ao BCE atribuições específicas no que diz respeito às políticas relativas à supervisão prudencial das instituições de crédito (Regulamento do MUS), o Regulamento (UE) n.º 468/2014 do Banco Central Europeu de 16 de abril de 2014, que estabelece o quadro de cooperação, no âmbito do Mecanismo Único de Supervisão, entre o BCE e as autoridades nacionais competentes e com as autoridades nacionais designadas (Regulamento-Quadro do MUS), e o Regulamento (UE) n.º 806/2014 do Parlamento Europeu e do Conselho de 15 de julho de 2014, que estabelece regras e um procedimento uniformes para a resolução de instituições de crédito e de certas empresas de investimento no quadro de um Mecanismo Único de Resolução e de um Fundo Único de Resolução bancária (Regulamento do MUR), preveem o respeito por garantias processuais fundamentais na adoção de decisões de supervisão e de resolução.

Com efeito, o n.º 1 artigo 22.º do Regulamento do MUS refere que "[a]ntes de tomar decisões de supervisão, (...) o BCE dá às pessoas que são objeto do procedimento a possibilidade de ser ouvidas. O BCE baseia as suas decisões apenas nas objeções sobre as quais as partes em causa tenham tido oportunidade de apresentar as suas observações". Estas garantias apenas não serão aplicadas se "forem necessárias medidas urgentes para evitar danos graves ao sistema financeiro. Neste caso, o BCE pode adotar uma decisão provisória e dá às pessoas em causa a possibilidade de serem ouvidas com a maior brevidade possível após ter tomado a sua decisão".

O n.º 2 do mesmo artigo prevê, ainda, que os direitos de defesa das pessoas que são objeto do procedimento devem ser plenamente acautelados durante a tramitação do processo. Estas pessoas têm "o direito de consultar o processo em poder do BCE, sob reserva do interesse legítimo de terceiros na proteção dos seus segredos comerciais. O direito de consulta do processo não é extensível a informações confidenciais". O n.º 2 refere, por fim, que "as decisões do BCE devem ser fundamentadas".

Também o artigo 33.º do Regulamento-Quadro do MUS, relativo à fundamentação das decisões de supervisão do BCE, estabelece que "a decisão de supervisão do BCE será acompanhada de uma indicação da respetiva fundamentação" (n.º 1), que deverá conter "os factos materiais e as razões jurídicas nos quais o BCE baseou a sua decisão de supervisão" (n.º 2). Sem prejuízo do disposto no artigo 31.º, n.º 4, do referido Regulamento, que permite ao BCE adotar uma decisão de supervisão sem uma audiência prévia da parte em casos de urgência, o n.º 3 do artigo 33.º acrescenta que "o BCE baseará a sua decisão de supervisão apenas em factos e objeções

relativamente aos quais as partes tenham tido a possibilidade de apresentar as suas observações".

Já no quadro do Mecanismo Único de Resolução (MUR), o Regulamento do MUR estabelece igualmente, no artigo 10.º, n.º 13, que as decisões tomadas pelo Conselho Único de Resolução (CUR) ou pelas autoridades de resolução no âmbito da avaliação da resolubilidade devem "ser fundamentadas quanto à avaliação ou determinação em questão" (alínea a)) e "indicar de que forma essa avaliação ou determinação cumpre o requisito de aplicação proporcionada (...)" (alínea b)). A fundamentação da decisão é, ainda, exigida nos artigos 12.º-D, n.º 8, relativamente a "qualquer decisão do CUR de impor um requisito mínimo de fundos próprios e passivos elegíveis", e 12.º-E, n.º 4, relativamente a "qualquer decisão do CUR de impor um requisito adicional de fundos próprios e passivos elegíveis". O Regulamento do MUR contém, ainda, disposições que obrigam à audição das pessoas sujeitas a qualquer decisão que imponha coimas e/ou medidas pecuniárias compulsórias e à garantia do respeito pelos direitos de defesa destas (artigo 40.º) e regras relativas ao acesso a documentos por parte dos sujeitos visados (artigo 90.º).

As decisões tomadas ao abrigo do Regulamento do MUR são passíveis de recurso, para a Câmara de Recurso criada para o efeito, ao abrigo do artigo 85.º do Regulamento, e, ainda, para o Tribunal de Justiça (artigo 86.º do Regulamento).

3.2. No contexto nacional

Devido à importância, às vantagens e aos riscos da inteligência artificial, assim como do restante desenvolvimento tecnológico, vários Estados, individualmente, têm encetado esforços na promoção e adoção de políticas de transição digital.

Neste âmbito, a nível nacional, salienta-se a Estratégia Nacional de Inteligência Artificial[119], publicada em 2019, tem como objetivo a promoção e mobilização da sociedade em geral para o ensino e investigação, para a inovação e desenvolvimento de produtos e serviços suportados em tecnologias de inteligência artificial, através, por exemplo, do financiamento para bolsas de doutoramento em projetos de investigação em IA e do desenvolvimento de uma plataforma — denominada PT AI WATCH — que permitirá o mapeamento de projetos relativos à inteligência artificial. Destaca-se, ainda, a publicação do Guia Para Uma Inteligência Artificial Ética, Transparente e Responsável na Administração Pública, sendo este um documento orientador de apoio a projetos de IA Responsável[120].

Seguiu-se a criação do Plano de Ação para a Transição Digital, aprovado em 2020 através de Resolução de Conselho de Ministros n.º 30/2020, de 21 de abril. Tal Plano encontra-se divido em três Pilares: (i) Pilar I — Capacitação e inclusão digital das pessoas; (ii) Pilar II — Transformação digital do tecido empresarial; e (iii) Pilar III - Digitalização do Estado.

Ainda a este propósito, destaca-se a Carta Portuguesa de Direitos Humanos na Era Digital, aprovada em 2021[121], onde se encontra consagrado o papel de Portugal na "transformação da Internet num instrumento de conquista de liberdade, igualdade e justiça social e num espaço de promoção, proteção e livre exercício dos direitos humanos, com vista a uma inclusão social

[119] Disponível em https://www.incode2030.gov.pt/aip-2030/.
[120] Disponível em Guia para uma Inteligência Artificial ética, transparente e responsável na Administração Pública.
[121] Lei n.º 27/2021, de 17 de maio.

em ambiente digital." (artigo 2.º, n.º 1). O artigo 8.º institui o direito à privacidade na era digital e o artigo 9.º enuncia as principais regras de utilização da IA, nomeadamente o respeito pelos direitos fundamentais e por princípios como a segurança e a transparência, estabelecendo que "as decisões com impacto significativo na esfera dos destinatários que sejam tomadas mediante o uso de algoritmos devem ser comunicadas aos interessados, sendo suscetíveis de recurso e auditáveis, nos termos previstos na lei" (n.º 2).

Assim, não só se verifica a criação de políticas de transição digital para todos os setores empresariais portugueses, como, igualmente, para a atividade da Administração Pública, nomeadamente nos setores da educação, da saúde e das infraestruturas.

Neste sentido, no que concerne à atividade das autoridades públicas, verifica-se que aquelas que recorram à utilização de ferramentas tecnológicas, em particular nos seus processos de tomada de decisão, devem necessariamente respeitar as garantias procedimentais afirmadas em princípios gerais de Direito Administrativo nacional.

No exercício de poderes públicos de autoridade, em particular no domínio do Direito Administrativo, o Banco de Portugal está igualmente sujeito a estes princípios.

A Lei Orgânica do Banco de Portugal (LOBP)[122] carateriza o Banco como uma pessoa coletiva de direito público (artigo 1.º). Como tal, dispõe a LOBP que, no exercício de poderes públicos de autoridade, são aplicáveis ao Banco de Portugal as disposições do Código do Procedimento Administrativo (CPA) e quaisquer outras normas e princípios de âmbito geral respeitantes aos atos administrativos do Estado (artigo 64.º, n.º 2, da LOBP).

Relevam, portanto, para a atuação do Banco de Portugal, vários princípios gerais da atividade administrativa[123], especialmente importantes no contexto da relação da Administração com os cidadãos. Tendo em conta estas exigências, a utilização de tecnologia pela Administração no exercício das suas funções públicas deverá ter em atenção o respeito pelos direitos e interesses que tais princípios visam proteger. Por essa razão, como referem alguns autores, "no Direito Administrativo esse receio passa (...) por exigir que os parâmetros valorativos (...) que conformam o procedimento administrativo equitativo sejam devidamente respeitados sempre que estiver em causa a utilização de tecnologia nesse mesmo procedimento"[124].

Considerando estas e outras questões, o novo CPA, aprovado pelo Decreto-Lei n.º 4/2015, de 7 de janeiro, registou inovações significativas quanto aos princípios gerais da atividade administrativa. Como é referido, desde logo, no preâmbulo do diploma de aprovação, foram incluídos no novo Código, entre outros, o princípio da boa administração, os novos princípios da responsabilidade (artigo 16.º), da administração aberta (artigo 17.º), da segurança de dados (artigo 18.º) e da cooperação leal da Administração Pública com a União Europeia (artigo 19.º), bem como princípios relativos à administração eletrónica (artigo 14.º). Em particular quanto a esta última, é sublinhado que se "pretende ir ao encontro da importância que os meios eletrónicos hoje assumem, tanto nas relações interadministrativas, como nas relações da Administração Pública com os particulares".

[122] Lei n.º 5/98, de 31 de janeiro, na redação atual.

[123] A doutrina descreve os princípios como "normas de conduta da Administração, que prescrevem condicionamentos substanciais aplicáveis às escolhas de conteúdos de ações administrativas", e que, como tal, operam como cânones com a função de orientar, condicionar e limitar a escolha de conteúdos de regulamentos, de contratos ou de decisões administrativas (Pedro Costa Gonçalves — Manual de Direito Administrativo, Volume 1. Coimbra: Almedina, 2019, página 374).

[124] Artur Flamínio da Silva — Inteligência Artificial e Direito Administrativo *in* Direito Administrativo e Tecnologia, 2.ª Edição. Coimbra: Almedina, 2021, página 14.

Assim, no artigo 14.º, o CPA estabelece, quanto à administração eletrónica, que "os órgãos e serviços da Administração Pública devem utilizar meios eletrónicos no desempenho da sua atividade, de modo a promover a eficiência e a transparência administrativas e a proximidade com os interessados" (artigo 14.º, n.º 1). Estes meios eletrónicos deverão "garantir a disponibilidade, o acesso, a integridade, a autenticidade, a confidencialidade, a conservação e a segurança da informação" (artigo 14.º, n.º 2).

A utilização de meios eletrónicos deverá situar-se, ainda, dentro dos limites estabelecidos na Constituição e na lei, estando sujeita às garantias previstas no referido Código e aos princípios gerais da atividade administrativa (artigo 14.º, n.º 3). Consagra-se, assim, neste artigo, "a paridade garantística entre as formas de exercício tradicional da atividade administrativa e as novas formas eletrónicas do agir administrativo"[125],[126]. Em particular, quanto à tomada de decisões pela Administração Pública, relevam alguns princípios gerais da atividade administrativa, entre os quais se destacam os seguintes:

- O princípio da decisão, previsto no artigo 13.º do CPA, impõe aos órgãos da Administração Pública o dever de se pronunciar "sobre todos os assuntos da sua competência que lhes sejam apresentados e, nomeadamente, sobre os assuntos que aos interessados digam diretamente respeito, bem como sobre quaisquer petições, representações, reclamações ou queixas formuladas em defesa da Constituição, das leis ou do interesse público". O n.º 3 deste artigo acrescenta, ainda, que os órgãos da Administração Pública podem decidir sobre coisa diferente ou mais ampla do que a pedida, quando o interesse público assim o exija;

- O princípio da fundamentação (consagrado constitucionalmente no artigo 268.º da Constituição da República Portuguesa (CRP)), presente no artigo 152.º do CPA (relativo ao dever de fundamentação nos atos administrativos), impõe, ainda, um dever de fundamentação de um conjunto alargado de atos administrativos, entre os quais se destacam os que afetem por qualquer modo direitos ou interesses legalmente protegidos ou imponham ou agravem deveres, os que decidam reclamação ou recurso, os que decidam em contrário de pretensão formulada por interessado ou de parecer, informação ou proposta oficial, e os que impliquem declaração de nulidade, anulação, revogação, modificação ou suspensão de ato administrativo anterior;

- O princípio da boa administração dispõe que a Administração Pública deve pautar-se por critérios de eficiência, economicidade e celeridade (artigo 5.º do CPA), exigindo, assim, que, além de conforme à lei e ao direito, os seus agentes devam agir como "bons administradores"[127];

- O princípio da adequação procedimental, consagrado no artigo 56.º do CPA, determina que, na ausência de normas jurídicas injuntivas, o responsável pela direção do procedimento goza de discricionariedade na respetiva estruturação, que, no respeito pelos princípios gerais da

[125] Artur Flamínio da Silva — Inteligência Artificial e Direito Administrativo, *op. cit.*, página 15.

[126] Veja-se que o artigo 61.º do CPA prevê a possibilidade de utilização de meios tecnológicos para facilitar e tornar mais simples a instrução de procedimentos. De modo a cumprir as devidas garantias legais e proteger a confiança dos interessados, nos artigos 61.º, 62.º e 64.º, n.º 3, são enunciadas várias características que os meios eletrónicos e o balcão único eletrónico deverão assegurar. Além disso, também a propósito do envio de notificações se promove a utilização de meios eletrónicos, mormente no artigo 112.º, n.º 1, alínea c). Não obstante, o n.º 2 do referido artigo estipula as circunstâncias em que será necessário obter o prévio consentimento do notificando para o efeito. Ainda por referência à possibilidade de implementar meios tecnológicos no contexto do procedimento administrativo, foram consagrados pelo legislador alguns requisitos para a notificação de atos administrativos, sendo estes aplicados à notificação por meios tecnológicos, por forma a cumprir com as garantias legalmente previstas.

[127] Pedro Costa Gonçalves — Manual de Direito Administrativo, *op. cit.*, página 106.

atividade administrativa, deve ser orientada pelos interesses públicos da participação, da eficiência, da economicidade e da celeridade na preparação da decisão;

- O princípio da colaboração com os particulares (artigo 11.º do CPA) e o princípio da participação (artigo 12.º do CPA) estabelecem que a Administração Pública deve, nomeadamente, prestar aos particulares as informações e os esclarecimentos de que careçam e assegurar a sua participação na formação das decisões que lhes digam respeito, designadamente através da respetiva audiência;
- O princípio da administração aberta (artigo 17.º do CPA) determina o direito de acesso aos arquivos e registos administrativos, cumpridas as condições legais, mesmo quando o procedimento não lhes diga diretamente respeito;
- O princípio da proteção dos dados pessoais (artigo 18.º do CPA) dispõe que os particulares têm direito à proteção dos seus dados pessoais e à segurança e integridade dos suportes, sistemas e aplicações utilizados para o efeito;
- O princípio da responsabilidade impõe à Administração Pública que responda, nos termos da lei, pelos danos causados no exercício da sua atividade (artigo 16.º do CPA).

No contexto da utilização de tecnologia em procedimentos administrativos, devem, ainda, considerar-se os desafios relativos à utilização de ferramentas para a execução de determinadas tarefas pelos órgãos da Administração Pública que são tradicionalmente executadas sem recurso a estas.

Ainda que com distinta influência e preponderância, o conteúdo dos princípios e regras acima referidos terá sempre de ser acautelado quando as autoridades públicas recorram, na sua atividade, à utilização de ferramentas de *Suptech*, em particular no âmbito de processos de tomada de decisão, de forma semelhante ao que é feito no domínio dos atos da Administração ditos "tradicionais", que não recorrem a ferramentas tecnológicas.

4 Desafios jurídicos e operacionais no âmbito da supervisão

Atendendo às considerações acima, a utilização de ferramentas de *Regtech* e *Suptech*, respetivamente por supervisionado e supervisor, trazem múltiplos benefícios e confirmam que ambos não estão indiferentes à digitalização do setor, mas que, pelo contrário, adotam estratégias com vista a acompanhar a evolução tecnológica e retirar dela os maiores benefícios. Não obstante, a implementação e utilização destas ferramentas acarretam diversos desafios, alguns dos quais já abordados *supra*. Assim, fica claro que, se, por um lado, a utilização destas ferramentas traz novas oportunidades, por outro lado, também gera novos desafios, decorrentes da natureza digital destas soluções, que deverão ser devidamente analisados e geridos.

O Banco de Portugal, como vimos, tem um papel preponderante nesta matéria, promovendo a sua própria transformação digital, com todos os desafios que lhe são inerentes, e buscando acompanhar a transformação digital das instituições. Analisemos, portanto, quais são os principais desafios, sobretudo de ordem jurídica, mas também de ordem operacional, que se colocam no contexto da atividade de supervisão.

4.1 Jurídicos

A. Integridade e acessibilidade dos dados

No que se refere aos desafios jurídicos, estes são, desde logo, evidentes em matéria de dados.

Como sabemos, "A informação é um recurso que tem valor essencial para as organizações, incluindo-se nesta aceção os Estados: é um valor decisivo e fundamental nos dias em que vivemos e assume um aspeto relevante na segurança e defesa das nações. Qualquer interrupção de serviço público, utilização indevida de informação classificada ou destruição de dados de cariz importante pode pôr em causa a confiança dos cidadãos, os interesses — e até a própria soberania — dos Estados"[128].

Ora, a evolução tecnológica e a digitalização do setor financeiro serviram de elemento "catalisador" de diversas mudanças relativamente ao acesso à informação e ao fluxo de dados. Os meios de armazenamento de dados, a granularidade dos dados fornecidos e o valor crescente que assumem tornam-nos mais apetecíveis e obrigam a reforçar a sua proteção. A salvaguarda da integridade dos dados é, nos dias que correm, um dos grandes desafios, para instituições e autoridades, sendo cada vez mais imperiosa[129].

Esta preocupação começou por ganhar mais destaque com o advento das *Fintech*, que passaram a ter acesso a uma grande quantidade de dados que as instituições tradicionalmente não tinham, o que se torna ainda mais evidente atualmente, com o fenómeno das *Bigtech*[130]. Por sua vez, a expansão da inteligência artificial e de todas as ferramentas relacionadas aconteceu devido à conjugação de fatores como o aumento da quantidade de dados, mencionado anteriormente, e das capacidades de computação, criando, assim, uma simbiose entre inteligência artificial e *data*[131].

Se, por um lado, a utilização destas ferramentas permite a extração e o tratamento massivo de dados e informações — recorde-se, aliás, que, conforme notado *supra*, as ferramentas de *Suptech* têm duas principais áreas de aplicação: recolha de dados (*data collection*) e análise de dados (*data analytics*) —, por outro lado, tal requer, por isso, cautelas adicionais. Em matéria de dados, são diversos os desafios que se colocam, de ordem operacional e jurídica, que vão desde a segurança dos dados à sua localização/armazenamento (podendo levantar temas *cross-*

[128] Ana Vaz – Segurança da Informação, Protecção da Privacidade e dos Dados Pessoais — Verão 2007, N.º 117 — 3.ª Série, página 39 (disponível em *nr-117_pdf.PMD (rcaap.pt)).

[129] Cfr. considerandos 6 e 7 do RGPD: "(6) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais. (7) Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas.".

[130] "Como sucedâneo relevante da sua atividade é o grande volume de dados dos utilizadores dos seus serviços. Isto deve-se a um contexto de elevadas capacidades de processamento e de armazenagem de software que tende a oferecer gamas de serviços relacionais que provocam efeitos trabalho em rede promovendo ciclos virtuosos." (Carlos Gonçalves — As Big tech como *players* do Sistema Financeiro. Dissertação de Mestrado, ISG, 2020 (disponível em https://comum.rcaap.pt/bitstream/10400.26/34109/1/Tese_Carlos_Gon%C3%A7alves_Vers%C3%A3o_Final.pdf)).

[131] Inês Oliveira e José Luís Dias — Inteligência Artificial e Proteção de Dados *in* Inteligência Artificial no Contexto do Direito Público: Portugal e Brasil, 1.ª Edição. Coimbra: Almedina, 2023, página 147.

border), qualidade[132] e transparência[133],[134], que requerem uma adequada estrutura de *governance* e outras cautelas adicionais.

A recolha, sistematização, tratamento e análise de dados feita através de ferramentas de *Suptech* poderá, desde logo nos casos em que envolva dados pessoais, obrigar a cautelas adicionais relativamente ao cumprimento de princípios e normas decorrentes da legislação europeia e nacional em matéria de proteção de dados pessoais[135], nas quais se incluem o Regulamento Geral sobre a Proteção de Dados (RGPD)[136] e o princípio da proteção dos dados pessoais, previsto no artigo 8.º da CDFUE e no artigo 18.º do CPA.

Importa atentar, sobretudo, ao processo de recolha dos dados, através do qual as autoridades poderão ter acesso a quantidades massivas de dados. Neste sentido, destacam-se os princípios da licitude, da lealdade e da transparência previstos no artigo 5.º, n.º 1, alínea a) do RGPD. De acordo com estes, a recolha e utilização de dados pessoais deve ser realizada com base numa causa de licitude, sendo necessária a promoção de um tratamento equitativo dos dados pessoais e o respeito pelos interesses e expectativas legítimos dos titulares de dados, assim como da transparência necessária ao longo de todo o processo. Assim, a utilização de ferramentas tecnológicas, mormente de inteligência artificial, encontra-se restringida pelas limitações e obrigações decorrentes das disposições do RGPD[137]. Na atividade das autoridades de supervisão, o processo de recolha dos dados necessários à prossecução das respetivas missões não deverá incluir o acesso a informações de caráter pessoal ou a informações sensíveis de caráter comercial, que devem permanecer de acesso vedado[138], a menos que sejam necessárias para o exercício da supervisão e exista habilitação legal para o efeito[139]. Tal como acontece no panorama atual, de forma a assegurar a proteção dos dados, as autoridades

[132] *"Suptech applications rely on machine-readable data – i.e. in a format that can be processed by computer programmes. As such, quality, standardisation and completeness of dataare key requirements and can pose major challenges, especially upon leveraging unstructured data collected from non-traditional sources of information (e.g. open source or social media)." (...) "Providing sufficient amounts of quality data to build machine learning applications can also be an issue. For instance, in relation to its Project Apollo, Singapore's MAS reported the scarcity of training data – particularly expert reports associated with prosecution outcomes – as a main challenge. Having a sufficient volume of such data is a key requirement to continually improve the accuracy and robustness of the algorithms, and to validate Apollo's models and methodologies in order for its results to be admissible for use in a court of law. Likewise, several law enforcement agencies involved in combatting corruption also identify data quality and standardisation as primary challenges for the effective use of AI, in particular for the detection and enforcement of corruption and foreign bribery offences. As such, it is important to ensure that information provided by companies to law enforcement authorities (either voluntarily through self-reporting and cooperation or under some form of compulsion) is in a format that authorities' systems can read. Standardisation is often obtained through protocols or guidance from the authorities themselves or by using industry standard protocols*" (OCDE — 5. The use of SupTech to enhance market supervision and integrity *in* OECD Business and Finance Outlook 2021: AI in Business and Finance (disponível em https://www.oecd-ilibrary.org/sites/d478df4c-en/index.html?itemId=/content/component/d478df4c-en).

[133] OCDE — 5. The use of SupTech to enhance market supervision and integrity.

[134] Cœuré warns of 'black box' problem for regulators - Central Banking.

[135] A cujo cumprimento o Banco de Portugal está obrigado (cf. Proteção de dados | Banco de Portugal (bportugal.pt)).

[136] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

[137] Note-se, a este respeito, que a autoridade francesa de proteção de dados ("CNIL") divulgou orientações oficiais sobre como deverá ser assegurado o cumprimento do RGPD na fase de desenvolvimento de um sistema de inteligência artificial (sem incluir, para já, a fase de implementação desses sistemas).

[138] "*This keen awareness of potential legal issues is reflected in OeNB's reporting solution. The solution is designed in such a way that OeNB has no direct access to the commercially sensitive raw data of the supervised banks since there is no legal basis for supervisors to have access to this data*" (BROEDERS, Dirk; PRENIO, Jeremy — Innovative technology in financial supervision (suptech) — the experience of early users. FSI Insights on policy implementation, No 9. 2018 (disponível em *Innovative technology in financial supervision (Suptech) — the experience of early users (bis.org)).

[139] A este respeito, *vide*, por exemplo, o artigo 120.º do RGICSF.

deverão garantir que dispõem das autorizações necessárias para a utilização de determinados dados para fins de supervisão[140],[141],[142].

Ademais, no que concerne à adoção de sistemas de "*push and pull*"[143] destaca-se que as autoridades deverão promover o acesso seguro a quantidades massivas de dados das instituições, tendo presentes todas as obrigações legais e responsabilidades a que o supervisor está adstrito, no decorrer da sua atividade.

Veja-se, ainda, a título de exemplo, a utilização de ferramentas de *Suptech* com tecnologia de registo distribuído (*distributed ledger technology*), que, ao oferecerem transparência e imutabilidade[144], podem trazer desafios ao cumprimento do RGPD, nos casos em que esteja em causa a utilização de dados pessoais, dado que este último prevê a capacidade de anonimizar e apagar dados pessoais e, também, relativamente às limitações de armazenamento nele previstas[145].

A localização/armazenamento dos dados pode também representar um desafio jurídico adicional na utilização de ferramentas de *Suptech*, podendo levantar questões *cross-border*, em particular (mas não apenas) dúvidas quanto às provas "digitais" e a investigações (as autoridades responsáveis pela aplicação da lei podem ver-se impossibilitadas de alargar os seus poderes de investigação aos dados localizados no estrangeiro[146]).

Refira-se, também, a interligação cada vez mais intensa entre regulados e reguladores, por um lado, e entre reguladores de várias áreas, por outro, cuja interligação poderá pôr em causa a exposição a grandes volumes de dados sensíveis e aumentar a vulnerabilidade do sistema a ameaças cibernéticas[147] (*vide* relativamente a esta matéria o ponto 4.2. b)).

Ademais, deverá acautelar-se que os dados pessoais inseridos nestas ferramentas não sejam utilizados para fins não pretendidos (por exemplo, deverá garantir-se que os dados não serão utilizados para treino das ferramentas).

Importa, assim, sobretudo, garantir que (i) os reguladores têm autorização para monitorizar, recolher e processar os dados através destas ferramentas, (ii) a utilização destas ferramentas não viola disposições do RGPD, nem os princípios que devem ser respeitados em matéria de dados pessoais, (iii) são definidas e respeitadas boas práticas em matéria de *governance*, de forma a garantir uma utilização responsável das ferramentas (é feita uma devida avaliação e análise de riscos) e (iv) o sistema é suficientemente resiliente para garantir a segurança e

[140] Dirk Broeders; Jeremy Prenio, — Innovative technology in financial supervision (suptech) — the experience of early users.

[141] Note-se, também, a importância da Lei n.º 26/2016, de 22 de agosto, isto é, a Lei de Acesso aos Documentos Administrativos ("LADA") que define um regime de acesso aos documentos administrativos que contêm dados pessoais, por parte de terceiros, sendo este acesso permitido se existir um interesse direto, pessoal, legítimo e constitucionalmente protegido considerado suficientemente relevante (artigo 6.º, n.º 5, alínea b)).

[142] "*Em diferentes graus, os bancos centrais e outros decisores políticos precisam de assegurar o público de que os dados não serão utilizados para violações injustificadas ou não autorizadas do direito à privacidade dos indivíduos.*" em Artigo de opinião do Administrador Hélder Rosalino no livro "88 Vozes sobre Inteligência Artificial" - A Inteligência Artificial ao serviço dos bancos centrais | Banco de Portugal (bportugal.pt)

[143] "*In the aim of improving data collection, some financial authorities have piloted the adoption of both 'push' and 'pull' technologies in recent years. While the former refers to pre-defined data being delivered from the regulated entity to the regulator, the latter enables the authority to draw data from the regulated entity as required*" (OCDE — 5. The use of SupTech to enhance market supervision and integrity).

[144] Consideram-se imutáveis porque não permitem a alteração unilateral por nenhuma das partes envolvidas.

[145] Emeline Denis; Daniel Blume — Using digital technologies to strengthen shareholder participation. Going Digital Toolkit Policy Note, No. 9, 2021 (disponível em Using digital technologies to strengthen shareholder participation (oecd.org)).

[146] OCDE — 5. The use of SupTech to enhance market supervision and integrity, ponto 5.4.2.

[147] *ESMA Report on Trends, Risks and Vulnerabilities, Financial innovation Regtech and Suptech — change for markets and authorities*, No 1, 2019. Página 45 (disponível em trv_2019_1-Regtech_and_Suptech_change_for_markets_and_authorities.pdf (europa.eu)).

proteção de dados e garantir a salvaguarda das informações cobertas por segredo de supervisão.

B. Subcontratação (*outsourcing*)

As autoridades, bem como as instituições supervisionadas, podem optar por ferramentas de *Suptech* desenvolvidas *in-house* mas também podem recorrera soluções externasO recurso a opções externas, do mercado, ou a uma combinação com soluções *in-house*, através da subcontratação, obriga a algumas cautelas.

Importa, desde logo, respeitar as Orientações da EBA sobre subcontratação (EBA/GL/2019/02), acima referidas, que devem ser cumpridas, quer pelas autoridades competentes, quer pelas instituições financeiras, e que preveem regras em matéria de governo interno (gestão de riscos, que incluem os decorrentes de contratos celebrados com terceiros). Preveem, a este respeito, que:

"A subcontratação de funções não pode resultar na delegação das responsabilidades do órgão de administração. As instituições e as instituições de pagamento continuam a ser inteiramente responsáveis pelo cumprimento de todas as suas obrigações regulamentares, incluindo a capacidade para supervisionar a subcontratação de funções essenciais ou importantes".

O Banco de Portugal comunicou à EBA a sua intenção de dar cumprimento a estas Orientações e transmitiu às instituições supervisionadas a importância do cumprimento dos requisitos nelas previstos, através da Carta Circular n.º CC/2019/00000065[148].

Assim, importa ter a consciência de que, muito embora as instituições possam recorrer à subcontratação, devem dispor das competências adequadas e de recursos suficientes para assegurar a gestão e supervisão dos acordos[149]. As autoridades competentes devem fazer essa avaliação e garantir que a subcontratação não impactará a supervisão efetiva das instituições em questão e que estas últimas, por sua vez, dispõem de mecanismos de governo sólidos e cumprem os requisitos regulamentares[150].

Veja-se, a título de exemplo, o que prevê o Aviso n.º 1/2022, em matéria de branqueamento de capitais e do financiamento do terrorismo, a respeito da subcontratação e tecnologia: relativamente à subcontratação, obriga a que sejam identificados e avaliados os concretos riscos de branqueamento de capitais e do financiamento do terrorismo associados à subcontratação de processos/serviços/atividades (artigo 16.º, n.º 5); relativamente à utilização de novas tecnologias, obriga a que a informação a este respeito seja contemplada no relatório de prevenção do branqueamento de capitais e do financiamento do terrorismo (artigo 83.º, n.º 3).

Ora, importa notar que as instituições deverão ter capacidade para cumprir as suas funções, independentemente do recurso a serviços externos, terão de ter conhecimento daquilo que lhes é exigível no plano regulatório e não se poderão desresponsabilizar por subcontratarem determinadas tarefas, conforme previsto, também, na 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, em matéria de *governance* (artigo 88.º e ss). O próprio RGICSF estabelece, em matéria de governo interno, que os órgãos de administração e de fiscalização das instituições de crédito definem, fiscalizam e são

[148] https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares/384090267_11.docx.pdf.
[149] Orientações da EBA relativas à subcontratação, ponto 37.
[150] *Idem*, título V.

responsáveis, no âmbito das respetivas competências, pela aplicação de sistemas de governo que garantam a gestão eficaz e prudente da mesma, assumindo responsabilidade pela instituição de crédito (artigos 115.º-A e ss.). O governo da sociedade e o sistema de controlo interno abrangem as atividades subcontratadas, sendo que o Aviso do Banco de Portugal n.º 3/2020 refere que o sistema de controlo interno abrange toda a instituição, incluindo, entre outros, as atividades subcontratadas (artigo 12.º, n.º 2), sendo esta matéria explicitada, nomeadamente, nos artigos 36.º e seguintes deste regulamento[151].

C. Tomada de decisão

A tomada de decisão com base em algoritmos e a utilização de ferramentas com algum grau de automaticidade podem levar-nos a questionar até que ponto é que as decisões assim adotadas, com recurso a estas ferramentas de *Suptech*, podem afetar a esfera jurídica dos indivíduos e se serão compatíveis com determinadas garantias constitucionais e princípios gerais de Direito Administrativo.

No plano europeu, a proposta de Regulamento IA traz algumas limitações à utilização destas ferramentas, conforme se destacou acima.

No plano nacional, importa atentar, desde logo, ao princípio da decisão, previsto no artigo 13.º do CPA, que nos diz, segundo Paulo Otero, que "toda a pretensão formulada junto da Administração Pública corresponde sempre a uma decisão, isto no sentido em que os órgãos administrativos têm o dever de se pronunciar sobre todos os assuntos da sua competência que lhe sejam apresentados"[152] (sublinhado nosso). Ora, numa situação limite ou extrema, a tomada de decisões com base em ferramentas de *Suptech*, nomeadamente através de ferramentas que recorram ao uso de inteligência artificial, sem qualquer intervenção humana, podem entender-se como não sendo dos órgãos administrativos (isto sem prejuízo de determinados atos materiais que integram um procedimento administrativo poderem ser praticados exclusivamente de forma automatizada, como é, por exemplo, o caso dos atos emitidos no âmbito do balcão eletrónico e das notificações, situações previstas no artigo 62.º, n.ºs 2 e 4, e no artigo 122.º, n.º 1, alínea c), do CPA, respetivamente).

Por sua vez, certas exigências do princípio da boa administração preveem que a atuação da Administração Pública deverá pautar-se por critérios de eficiência, economicidade e celeridade. Ora, a ação administrativa deve então, conforme entende Pedro Costa Gonçalves, "orientar a sua ação de modo a obter os resultados pretendidos mediante a mobilização do mínimo possível de recursos"[153], buscando-se assim uma otimização dos recursos disponíveis, porém com garantias de uma atuação eficiente. O que se pretende, de acordo com Carlos Vieira de Almeida, e em respeito também pelo princípio da eficiência, é que se evitem trâmites desnecessários ou excessivamente complicados, comportamentos dilatórios e decisões inúteis[154]. As ferramentas de *Suptech* poderão tornar as decisões mais céleres e eficientes, importa, porém, garantir o equilíbrio entre celeridade e qualidade das informações ou decisões. A utilização de ferramentas que utilizem inteligência artificial ou *machine-learning* pode tornar mais fácil a análise de determinados dados e permitir o processamento de uma quantidade

[151] Veja-se, ainda, a este respeito, as normas habilitantes previstas no RGICSF em matéria de subcontratação: a respeito das obrigações de registo — artigo 99.º, n.º 2, do RGICSF, com remissão para artigo 17.º, n.º 1, alínea f); a respeito das obrigações de comunicação — artigo 120.º, n.º 1, alínea g) e n.º 2; e, relativa a supervisão em base consolidada — artigo 133.º, alínea c).

[152] Paulo Otero, — Direito do Procedimento Administrativo, Volume I. Coimbra: Almedina, 2016, página 110.

[153] Pedro Costa Gonçalves — Manual de Direito Administrativo, *op. cit.*, página 401.

[154] José Carlos Vieira de Andrade — A justiça administrativa. Coimbra: Almedina, 2016, página 448.

massiva de dados, encontrando padrões de dados impercetíveis à análise humana. No entanto, pode fragilizar a qualidade das informações ou das análises (gerando, entre outros, riscos de enviesamento[155]) e os direitos de defesa das partes, em particular no que se refere à garantia de acesso e percetibilidade da fundamentação das decisões tomadas.

Refira-se ainda o princípio da colaboração com os particulares e da participação, previstos nos artigos 11.º e 12.º do CPA, respetivamente. Segundo o primeiro princípio, os órgãos da Administração Pública "devem atuar em estreita colaboração com os particulares, cumprindo-lhes, designadamente, prestar aos particulares as informações e os esclarecimentos de que careçam" — o que pode tornar-se particularmente desafiante quando sejam utilizadas ferramentas tecnológicas. A este propósito, refira-se ainda que tal implica, como dispõe o n.º 2 do artigo 11.º, que "a Administração Pública é responsável pelas informações prestadas por escrito aos particulares, ainda que não obrigatórias".

No se refere ao segundo princípio, procura-se sempre promover a participação da pessoa coletiva ou individual no processo decisório, aprofundando-se os princípios da transparência (artigo 17.º do CPA) e da confiança, transversais ao procedimento administrativo, sendo de considerar, neste contexto, nomeadamente, um certo grau de "desconfiança" relacionada com os programas informáticos. Verifica-se uma tendência de crescente substituição da decisão unilateral pela decisão negociada com os cidadãos afetados[156]. A utilização de ferramentas de *Suptech* poderá trazer desafios adicionais a este respeito, decorrentes, nomeadamente, de eventuais dificuldades na promoção da participação da pessoa coletiva ou individual no processo decisório.

Conforme mencionado *supra*, a transparência é fulcral em qualquer procedimento administrativo. Como tal, o princípio da transparência encontra-se claramente consagrado nos ordenamentos jurídicos nacional e europeu, através do CPA, no seu artigo 17.º, e do artigo 42.º da CDFUE (direito de acesso aos documentos). A utilização de ferramentas de *Suptech* apresenta, no entanto, vários desafios ao respeito pelo referido princípio. A utilização de programas que recorrem ao uso de inteligência artificial, por exemplo, poderá tornar o processo decisório e a própria decisão obscura e ininteligível, nomeadamente se não existir intervenção humana[157], [158]. Destaca-se, a este propósito, a utilização, em alguns modelos de *machine-learning*, de algoritmos

[155] "O outro grande ponto de discussão quando se aborda ética e inteligência artificial, já referido anteriormente, é a o enviesamento (bias), e como se garante que os sistemas se mantêm "justos" ou "neutros". Este tema estará sempre muito dependente dos dados usados, sendo necessário investir em abordagens para identificar esses enviesamentos na vertente técnica. Mas será, também, necessário definir orientações e princípios para a transparência, responsibilização e justiça na utilização desses sistemas, assegurando a sua conformidade através de auditorias aos dados e modelos, de testes às aplicações e, não menos importante, pela atualização oportuna das normas definidas de modo a adequá-la a novas realidades." em Artigo de opinião do Administrador Hélder Rosalino no livro *88 Vozes sobre Inteligência Artificial — A Inteligência Artificial ao serviço dos bancos centrais* | Banco de Portugal (bportugal.pt)

[156] João Caupers; Vera Eiró, — Introdução ao Direito Administrativo, 12.ª Edição. Ancora Editoras, páginas 96–97.

[157] *"(...) transparency around algorithmic decisions is sometimes limited by things like corporate or state secrecy or technical literacy. Machine learning further complicates this since the internal decision logic of the model is not always understandable, even for the programmer. While the learning algorithm may be open and transparent, the model it produces may not be. This has implications for the development of machine learning systems, but more importantly for its safe deployment and accountability." Artificial Intelligence and Machine Learning: Policy Paper*, *Internet Society*, *April* 2017 (disponível em Artificial Intelligence & Machine Learning: Policy Paper | Internet Society).

[158] Neste sentido, o artigo 22.º do RGPD consagra a proibição de decisões individuais automatizadas, salvo algumas exceções, como por exemplo se "a decisão for autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados". Todavia, o n.º 1 do artigo 22.º, como se encontra construído, apresenta algumas limitações como o facto de apenas se aplicar a pessoas individuais e, portanto, não a pessoas coletivas, e apenas a decisões que não possuam qualquer tipo de intervenção humana no decorrer do processo (Francisca Almeida, — Inteligência Artificial e Atividade Administrativa: notas breves sobre automatização na emissão de atos administrativos *in* Revista de Direito Administrativo. Lisboa: AAFDL Editora, 2023, página 139).

não supervisionados, ou seja, de dados que não são previamente rotulados, pretendendo-se, assim, que o algoritmo detete características similares entre um conjunto de dados e, consequentemente, padrões[159]. Uma vez que o algoritmo deteta estes padrões autonomamente, poderá ser difícil a explicação do caminho lógico realizado para chegar àquele resultado específico, o que também releva para o dever de fundamentação das decisões, conforme abaixo se considera[160].

A Administração poderá, inclusivamente, ver-se confrontada com pedidos de acesso a dados ou algoritmos relacionados com as ferramentas de *Suptech* utilizadas no âmbito da adoção de decisões administrativas (*vide* a este respeito o ponto 4.1. a)). Sem prejuízo, sendo que estes instrumentos, além de um elevado grau de complexidade, pressupõem conhecimentos extensos, mesmo que a informação seja concedida ao requerente, poderão suscitar-se desafios quanto à sua capacidade de compreender e analisar os dados em causa[161]. Surge, assim, o problema habitualmente intitulado de "*black-box problem*"[162],[163].

Nesta senda, a "*eXplainable AI* (XAI)" poderá ter um papel preponderante, ao procurar sumariar as razões para determinada tomada de decisão – criando assim condições para se tirar o maior proveito destas ferramentas, trazendo maior segurança e transparência quanto à sua utilização[164,165], permitindo ainda outros ganhos[166]. Ainda de forma a ultrapassar algum grau de opacidade derivado, por exemplo, de direitos relativos a propriedade intelectual ou direitos de autor[167], a criação e desenvolvimento, pelas autoridades, das suas próprias ferramentas tecnológicas poderá ser uma das soluções[168].

Contudo, note-se que, uma vez que a "linguagem jurídica" não se poderá definir como fixa, as suas variantes interpretativas e mutabilidade conceptual criam um desafio extra à sua aplicação maquinal. A aplicação de fórmulas algorítmicas aos dados jurídicos cria desafios quanto à

[159] The Royal Society — Explainable AI: the basics. 2019, página 6 (disponível em: royalsociety.org).

[160] Francisca Almeida, *op.cit.*, página 138.

[161] "Este tipo de modelos utiliza um conjunto de base de dados e não explicam o seu raciocínio, sendo por vezes obscuro o processo de tomada de decisão. Mesmo os próprios criadores poderão não conseguir explicar, na totalidade, o funcionamento do modelo" (Council of the European Union – "*ChatGPT in the Public Sector – overhyped or overlooked?*" 24 April, 2023, página 10).

[162] A este respeito, veja-se a entrevista dada por CŒURÉ Benoît para a Central Banking Newsdesk "*Cœuré warns of 'black box' problem for regulators*", em 19 de Agosto de 2020 (disponível em Cœuré warns of 'black box' problem for regulators — Central Banking.

[163] "*challenges such as the black-box problem might require supervisors to 'leave their comfort zone' and adopt new methods. This would partly require 'breaking the silos' of financial regulation, he said, and also the creation of a 'multidisciplinary dialogue' with broader regulators, such as those that oversee telecoms. Cœuré noted there was a tension for supervisors in adopting new technology, as a degree of uncertainty, experimentation and a 'fail-fast mindset' tended to be needed. 'I think we can agree these attributes do not always sit comfortably with prudent supervisors and risk-minded financial institutions'" New forms of collaboration could be part of the solution, Cœuré argued* (...))" (Cœuré warns of 'black box' problem for regulators - Central Banking).

[164] Tal como destacado num artigo disponibilizado pela McKinsey "*As artificial intelligence informs more decisions, companies' AI systems must be understood by users and those affected by AI use. Actions in two areas can maximize AI's benefits and minimize risk.*" (Explainable AI: Getting it right in business | McKinsey)

[165] "A literatura recente tem explorado mecanismos para interpretar resultados derivados de modelos de machine learning, contribuindo para um novo campo de investigação denominado eXplainable AI (XAI). Trata-se de uma abordagem que se concentra em tornar os modelos e sistemas de inteligência artificial mais compreensíveis e transparentes para os seres humanos evitando as tais "caixas negras" que dificultam ou impossibilitam perceber como chegam às suas conclusões ou tomam as decisões. Isso pode ser problemático em muitas situações, especialmente em áreas em que a transparência e a explicabilidade são importantes, como em questões legais, éticas ou de segurança." em Artigo de opinião do Administrador Hélder Rosalino no livro "88 Vozes sobre Inteligência Artificial" — A Inteligência Artificial ao serviço dos bancos centrais | Banco de Portugal (bportugal.pt)

[166] Alguns dos quais mencionados no em outro artigo da McKinsey "*Five ways explainable AI can benefit organizations*", entre os quais "increasing productivity"; "*building trust and adoption*"; "*surfacing new, value-generating interventions*"; "*ensuring AI provides business value*"; "*mitigating regulatory and other risks*" (Explainable AI: Getting it right in business | McKinsey)

[167] Henrique Sousa Antunes - Direito e Inteligência Artificial, UCP Editora, 2020, pp. 39 e 40.

[168] Francisca Almeida, *op.cit.*, página 143.

(in)capacidade de interpretar convenientemente uma ciência social que se tem por uma textura aberta[169], como referia Hart.

Por fim, considere-se ainda o dever de fundamentação, previsto no artigo 152.º do CPA e no artigo 296.º, segundo parágrafo, do TFUE, e decorrente, igualmente, do princípio geral da boa administração.

Daqui resulta a necessidade de uma fundamentação expressa, que inclua as razões de facto e de direito, dos atos administrativos. Ora, pode colocar-se a questão de saber se uma decisão tomada com recurso a ferramentas de *Suptech*, que auxiliem o processo de tomada de decisão, apresentará dificuldades adicionais no que diz respeito à necessidade de promover e transmitir uma fundamentação adequada e completa das decisões, uma vez que, muitas vezes, os critérios por estas utilizados não serão tão facilmente percetíveis para o visado (não descurando o importante papel que a "*Explainable AI*" poderá ter neste âmbito, conforme acima notado).

Nesse sentido, dificilmente uma fundamentação adequada poderá ser elaborada sem intervenção humana, principalmente em procedimentos mais complexos ou que envolvem um maior grau de discricionariedade da parte da entidade administrativa. Ainda assim, poderá admitir-se que, em procedimentos muito simples, como a validação de certos reportes, por exemplo, a fundamentação possa ser essencialmente formulada pela ferramenta *Suptech*.

Por outro lado, o recurso (mais intensivo) a ferramentas de *Suptech*, que se distinguem, sobretudo, pela capacidade de identificar *outliers*, traçar padrões gerais de comportamento ou promover análises transversais com base em determinada tecnologia (e.g. *sentiment analysis*), pode trazer desafios adicionais ao dever de diligência, que sublinha a importância do caso concreto e da ponderação de elementos específicos de cada situação pela Administração[170]. Por outras palavras, as ferramentas de *Suptech*, de um modo geral, ajudam-nos a lidar com os "grandes números" e com a complexidade social e económica, mas dizem-nos pouco, à partida, pelo menos no seu estado atual de desenvolvimento, sobre as especificidades do caso concreto e, em todo o caso, poderão não ter a capacidade de promover uma avaliação mais valorativa quanto ao modo como os casos específicos devem ser tratados e decididos, e não dispensam a avaliação humana. Com efeito, este reduto mais humano e subjetivo do processo de análise e decisão não deverá ser eliminado, sendo fundamental para dar cumprimento ao dever de diligência, além de ser um passo necessário para promover a justificação adequada das decisões, que têm de ser compreensíveis, coerentes e transparentes, à luz da linguagem comum que utilizamos[171].

Procura-se, aqui, fomentar a transparência da decisão e da Administração, na sua atuação diária, dando a possibilidade ao cidadão requerente de compreender os motivos que levaram àquela deliberação, assistindo-lhe, naturalmente, se este não concordar com a decisão, o direito de recorrer da mesma (artigo 152.º do CPA e artigo 41.º, n.º 2, alínea c), da CDFUE).

Na verdade, importa ainda analisar, neste âmbito, a possibilidade, ou não, de existência de uma de delegação de poderes a ferramentas tecnológicas que tomem decisões de forma autónoma. Veja-se o artigo 36.º, n.º 1, do CPA que determina a irrenunciabilidade e inalienabilidade da

[169] H.L.A Hart — O Conceito de Direito (A. Ribeiro Mendes, trans.). Fundação Calouste Gulbenkian. Páginas 137-149.

[170] Luís Filipe Antunes — Decisão Automatizada baseada em inteligência artificial: utopia ou distopia? *in* Cadernos de Justiça Administrativa, 152, Centro de Estudos Judiciários do Minho, 2022, p. 60.

[171] Veja-se, por exemplo, a respeito do ChatGPT "*In the absence of clear regulation on ChatGPT accountability, humans are needed to monitor output especially when considering what lies ahead. And only humans can provide the personalised services, flexibility, emotional intelligence, and critical thinking needed to fulfil the requirements of public service*" (Council of the European Union – "*ChatGPT in the Public Sector – overhyped or overlooked?*" 24 April, 2023, página 1).

competência dos órgãos administrativos, salvo nos casos em que a delegação de poderes, a suplência e a substituição são permitidas, não estando prevista a possibilidade de delegação de poderes, suplência ou substituição a ferramentas tecnológicas, nos termos previstos no CPA (poderiam configurar um caso destes, por exemplo, as situações em que a decisão final de um procedimento administrativo fosse tomada por uma ferramenta tecnológica, sem a existência de uma confirmação ou validação final da mesma por parte do órgão administrativo competente). Note-se que, ao abrigo do CPA, é nulo o ato praticado sem competência (artigo 161.º, n.ºs 1 e 2, alíneas a) e b), do CPA). É certo que a delegação de poderes pressupõe autonomia e capacidade de atuação, pelo que entendemos excessivo este paralelo, em particular pela ausência de personalidade jurídica[172] destas ferramentas (condição essencial para a existência, como atualmente configurada, de uma delegação de poderes).

Além disso, veja-se que os artigos 44.º e seguintes apontam nessa direção, afirmando que a delegação de poderes só poderá ser realizada de um órgão administrativo para outro órgão ou agente da mesma pessoa coletiva ou outro órgão de diferente pessoa coletiva que pratique atos administrativos sobre a mesma matéria (artigo 44.º, n.º 1, do CPA), sendo que, conforme é possível ler no n.º 2 do artigo 44.º, o agente é aquele que, a qualquer título, exerça funções públicas ao serviço da pessoa coletiva. Deste modo, atendendo-se à letra da lei, compreende-se esta delegação apenas poderá ser realizada num órgão administrativo e num agente, não se incluindo, assim, no conceito de "agente" uma ferramenta tecnológica.

Contudo, parece-nos verdadeiramente questionável, uma vez que não existe uma verdadeira delegação (em termos jurídicos) e tal poderia trazer desafios adicionais ao cumprimento de outras normas e princípios administrativos, entre os quais os princípios da transparência, do inquisitório, da decisão, da adequação procedimental ou da participação e da colaboração com particulares.

D. Responsabilidade

Conforme destacado ao longo do presente estudo, a utilização de ferramentas de *Suptech* apresenta várias vantagens, nomeadamente em termos de celeridade e eficiência. Não obstante, muitas questões são suscitadas quando se estuda a sua utilização e respetivos impactos.

Na criação e desenvolvimento de ferramentas de *Suptech* questiona-se, em particular, quem será o responsável pela eventual utilização ou funcionamento erróneos de tais meios. Será exclusivamente o fornecedor da ferramenta, a entidade administrativa que contratou tais serviços, ou ambos?

No ordenamento jurídico português, o artigo 16.º do CPA, que consagra o princípio da responsabilidade, estabelece que "a Administração Pública responde, nos termos da lei, pelos danos causados no exercício da sua atividade".

Em particular, a responsabilidade civil extracontratual do Estado e das demais pessoas coletivas de direito público por danos resultantes do exercício da função administrativa rege-se nos termos do disposto no Regime da Responsabilidade Civil Extracontratual do Estado e demais entidades públicas ("RRCEE", aprovado pela Lei n.º 67/2007, de 31 de dezembro) (artigo 1.º, n.º

[172] Neste âmbito, colocam-se diversas questões, tendo, aliás a Comissão Europeia chegado a admitir a possibilidade de se atribuir/criar um "tipo de personalidade jurídica" ("personalidade jurídica eletrónica") aos *robots*, defendida, aliás, por alguns e questionada por outros, estes últimos sustentando que se deve atribuir tratamento equivalente às "coisas", por exemplo. Esta posição da Comissão Europeia foi, porém, alvo de críticas por grande parte da doutrina, nada se defendendo a este respeito, nem no Livro Branco, nem no Regulamento IA — conforme notado no seguinte artigo da Prof.ª Sónia Moreira "IA e Robótica: A caminho da personalidade jurídica" — (*2022_IA-E-ROBOTICA.pdf (uminho.pt))

1)[173]. O n.º 2 do artigo 1.º esclarece que se incluem no âmbito da responsabilidade civil extracontratual por danos resultantes do exercício da função administrativa "as ações e omissões adotadas no exercício de prerrogativas de poder público ou reguladas por disposições ou princípios de Direito Administrativo".

No caso do Banco de Portugal, ao atuar no exercício das suas prerrogativas de autoridade pública, aplica-se o disposto no RRCEE no âmbito da responsabilidade civil extracontratual por danos decorrentes do exercício da função administrativa.

No contexto do exercício desta função, o RRCEE distingue entre a responsabilidade por facto ilícito (artigos 7.º a 10.º) e a responsabilidade pelo risco (artigo 11.º). Assim, de acordo com o n.º 1 do artigo 7.º do RRCEE, "o Estado e as demais pessoas coletivas de direito público são exclusivamente responsáveis pelos danos que resultem de ações ou omissões ilícitas, cometidas com culpa leve, pelos titulares dos seus órgãos, funcionários ou agentes, no exercício da função administrativa e por causa desse exercício". O n.º 3 deste artigo acrescenta que estes serão, igualmente, "responsáveis quando os danos não tenham resultado do comportamento concreto de um titular de órgão, funcionário ou agente determinado, ou não seja possível provar a autoria pessoal da ação ou omissão, mas devam ser atribuídos a um funcionamento anormal do serviço". Nos termos do n.º 4 do mesmo artigo, existirá um "funcionamento anormal do serviço quando, atendendo às circunstâncias e a padrões médios de resultado, fosse razoavelmente exigível ao serviço uma atuação suscetível de evitar os danos produzidos".

De acordo com o artigo 8.º do RRCEE, o Estado e as demais pessoas coletivas de direito público são, ainda, responsáveis de forma solidária com os respetivos titulares de órgãos, funcionários e agentes, pelas ações ou omissões ilícitas por eles cometidas com dolo ou com diligência e zelo manifestamente inferiores àqueles a que se encontravam obrigados em razão do cargo, se estas tiverem sido cometidas no exercício das suas funções e por causa desse exercício (n.ºs 1 e 2).

Quanto à responsabilidade pelo risco, o n.º 1 do artigo 11.º prevê que o Estado e as demais pessoas coletivas de direito público respondam "pelos danos decorrentes de atividades, coisas ou serviços administrativos especialmente perigosos, salvo quando, nos termos gerais, se prove que houve força maior ou concorrência de culpa do lesado, podendo o tribunal, neste último caso, tendo em conta todas as circunstâncias, reduzir ou excluir a indemnização".

Assim construída, a responsabilidade civil extracontratual das entidades públicas, incluído as autoridades de supervisão, por danos decorrentes do exercício da função administrativa, engloba as ações e omissões no exercício de prerrogativas de poder público, ou reguladas por disposições ou princípios de direito administrativo, praticadas pelos titulares dos seus órgãos, funcionários ou agentes (inclusive através da utilização de ferramentas *Suptech*).

De igual forma, é importante notar que estão, ainda, abrangidas pelo disposto no RRCEE, quanto à sua responsabilidade civil, as pessoas coletivas de direito privado e respetivos trabalhadores, titulares de órgãos sociais, representantes legais ou auxiliares, por ações ou omissões que adotem no exercício de prerrogativas de poder público ou que sejam reguladas por disposições ou princípios de Direito Administrativo (artigo 1.º, n.º 5).

Sem prejuízo do exposto, importa, porém, ressalvar que estes diplomas, bem como a responsabilidade neles consagrada, refletem um contexto temporal e tecnológico onde não se colocava, ainda, a possibilidade de uma realidade em que as entidades públicas recorressem a

[173] Segundo o artigo 1.º, n.º 1, do RRCEE, as suas disposições abrangem a responsabilidade civil extracontratual do Estado e das demais pessoas coletivas de direito público por danos resultantes do exercício, tanto da função legislativa, como jurisdicional e, ainda, administrativa.

meios tecnológicos auxiliares da ação administrativa, e, em última instância, "substitutos" de pessoas singulares.

No mesmo sentido, ao nível do Direito da UE, dispõe o artigo 41.º, n.º 3, da CDFUE, relativo ao direito a uma boa administração, que "todas as pessoas têm direito à reparação, por parte da União, dos danos causados pelas suas instituições ou pelos seus agentes no exercício das respetivas funções, de acordo com os princípios gerais comuns às legislações dos Estados-Membros".

No plano do direito europeu e no que se refere à responsabilidade pelo recurso a ferramentas de IA, é particularmente relevante a Diretiva Responsabilidade IA, atualmente em negociação.

Como referido anteriormente, a Diretiva Responsabilidade IA propõe estabelecer requisitos uniformes para certos aspetos da responsabilidade civil extracontratual por danos causados pelo envolvimento de sistemas de IA, visando uma harmonização mínima nesta matéria. As suas disposições serão aplicáveis a ações de indemnização de direito civil extracontratual por danos causados por um sistema de IA, sempre que tais ações sejam intentadas ao abrigo de regimes de responsabilidade culposa (que preveem a responsabilidade legal de indemnizar os danos causados intencionalmente ou por ação ou omissão negligente).

Como referido anteriormente, estas normas aplicam-se aos fornecedores e utilizadores de sistemas de IA (artigo 3.º, n.º 1), que poderão ser tanto entidades públicas como privadas, sendo possível, assim, concluir que, no quadro da referida proposta de Diretiva, também as autoridades públicas, estarão sujeitas às regras quando recorram a este tipo de sistemas no exercício da sua atividade.

4.2 Operacionais

A. Riscos de concentração

Um dos riscos de ordem operacional é o risco de concentração numa única entidade/fornecedor de *Regtech* e *Suptech*. Se, por um lado, a concentração pode ser benéfica para assegurar um certo nível de uniformização e estandardização, por outro lado, um erro numa determinada ferramenta poderá passar a implicar um erro generalizado e de mais difícil identificação, gerando assim um risco sistémico, de contaminação de todo o sistema[174]. Porém, se, para evitar este risco de concentração, os supervisores no espaço da UE utilizarem diferentes fornecedores de *Suptech* — o que, aliás, tem sido uma realidade (*vide supra*) —, essa situação pode criar algumas discrepâncias e inconsistências na interpretação dos termos legais aplicáveis e diferentes abordagens seguidas por diferentes supervisores relativamente às mesmas regras[175].

[174] Refere o considerando 3) do Regulamento DORA que "o Comité Europeu do Risco Sistémico ("CERS") reafirmou, num relatório de 2020 sobre o ciber-risco sistémico, que o elevado nível de interligação existente entre as entidades financeiras, os mercados financeiros e as infraestruturas do mercado financeiro, e, em especial, as interdependências dos seus sistemas de TIC, poderiam constituir uma vulnerabilidade sistémica, porque os ciberincidentes localizados poderiam rapidamente propagar-se a partir de qualquer uma das aproximadamente 22 mil entidades financeiras da União a todo o sistema financeiro, sem qualquer entrave geográfico. As violações graves no domínio das TIC que ocorrem no setor financeiro não afetam unicamente as entidades financeiras, de forma isolada. Abrem também caminho à propagação de vulnerabilidades localizadas nos canais de transmissão financeiros e podem desencadear consequências negativas para a estabilidade do sistema financeiro da União, gerando, nomeadamente, crises de liquidez e uma perda de confiança geral nos mercados financeiros".

[175], Nuno Saldanha de Azevedo — *SupTech*: *A potential supervisory tool of European Banking Supervisors*, página 24 (disponível em SSRN-id3861890.pdf (sharepoint.com)).

Adicionalmente, a concentração num único fornecedor poderá também gerar ou aumentar o ciber-risco (a este propósito, veja-se o ponto 4.2. b)).

O risco de concentração traz consigo também um risco de "*gaming the system*", i.e., de utilização das regras e procedimentos que se conhecem da ferramenta, não para sua utilização proveitosa, mas para efeitos de manipulação do sistema para um resultado desejado, enviesando-o. Conforme notado pela *European Securities and Markets Authority* ("ESMA"):

"*One risk that authorities should bear in mind when developing automated detection tools is the possibility that malicious agents may learn to frustrate the tools by adapting their behaviour. For instance, market participants could, in theory, learn what types of behaviours are likely to cause a flag in a Suptech monitoring system. Using such information, firms might be able to structure their regulatory returns in such a way as to remain undetected. Separately, as firms develop their expertise in Regtech, their systems may become able to identify potential regulatory loopholes*"[176].

B. Ciber-riscos

A intensificação da utilização da tecnologia e da dependência em relação a esta resulta num aumento do risco cibernético. O crescimento dos ataques informáticos[177] tem vindo a colocar todo o setor financeiro em situação de alerta, sendo visto, inclusive, como uma verdadeira ameaça à estabilidade financeira e ao sistema financeiro como um todo. A recolha e tratamento de dados através de ferramentas de *Regtech* e *Suptech* aumenta o risco de exposição a eventuais ataques de *hackers*, podendo comprometer, assim, a segurança e privacidade dos dados e colocar em causa o cumprimento regulatório e o desempenho da atividade de supervisão. Ademais, o recurso a estas ferramentas no cumprimento da regulação e no exercício da atividade de supervisão para os fins acima descritos, com todos os benefícios que daí se podem retirar, aumenta a dependência tecnológica das autoridades e instituições e a necessidade de reforço da resiliência digital, uma vez que, quanto maior a dependência digital/tecnológica, maior o risco de ciberataques.

Assim, é imperativo que as autoridades e instituições reforcem a robustez dos seus sistemas informáticos a fim de mitigar a exposição a ciberataques e dispor de ferramentas adequadas para reagir e controlar os efeitos potenciais que deles decorrem. Deverão, ainda, prever a criação de sistemas de apoio protegidos capazes de assegurar que os supervisores continuem a desempenhar as suas funções independentemente da ocorrência de qualquer incidente cibernético[178]. Veja-se, ainda, que as fortes interligações financeiras e tecnológicas, que aumentam com a utilização destas ferramentas, podem fazer com que um ataque a uma instituição e/ou autoridade ou a um sistema ou serviço central utilizado por várias entidades possa rapidamente alastrar-se a todo o sistema financeiro, causando uma perturbação generalizada e perda de confiança[179]. Nesta senda, importa, também, não negligenciar a

[176] *ESMA Report on Trends, Risks and Vulnerabilities*, *Financial innovation Regtech and Suptech — change for markets and authorities* (disponível em trv_2019_1-Regtech_and_Suptech_change_for_markets_and_authorities.pdf (europa.eu)).

[177] "Isto coincide com os dados do Fundo Monetário Internacional (FMI), que alertou há uns meses que o número de ciberataques tinha triplicado na última década, e que a indústria dos serviços financeiros continua a ser o alvo preferido: de acordo com os dados recolhidos pela instituição, em 2020 houve cerca de 1500 ciberataques a bancos, enquanto que em 2012 houve cerca de 400.", Ana Paula — Serão as redes dos serviços financeiros seguras?, 24 de agosto 2021 (disponível em Os riscos de cibersegurança que os serviços financeiros enfrentam | WatchGuard Blog).

[178] Nuno Saldanha de Azevedo, — *SupTech*: *A potential supervisory tool of European Banking Supervisors*, página 25 (disponível em SSRN-id3861890.pdf (sharepoint.com)).

[179] Jennifer Elliott; Nigel Jenkinson — *Cyber Risk is the New Threat to Financial Stability*, 7 de dezembro de 2020 (disponível em Cyber Risk is the New Threat to Financial Stability (imf.org)).

necessidade dos fornecedores de serviços de *cloud*, entre outros, reforçarem igualmente a sua resistência e resiliência digital, para não gerarem riscos para o sistema.

Torna-se essencial criar um ecossistema resiliente, com processos robustos de gestão de risco das TIC e o menos vulnerável possível.

Estas preocupações e objetivos são partilhados e enfrentados: (i) no plano europeu, onde se destaca a este respeito, , a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva NIS, o Regulamento DORA, que integra o pacote de financiamento digital, conforme acima referido, e ainda as Orientações emitidas pela EBA relativas à gestão dos riscos associados às TIC e à segurança; e (ii) no plano nacional, nomeadamente, através do Decreto-Lei n.º 65/2021, de 30 de julho, que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança ("DL n.º 65/2021"), da Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016 (Diretiva NIS), e do Decreto-Lei n.º 20/2022, de 28 de janeiro, que aprova os procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas críticas nacionais e europeias.

No plano europeu, o Regulamento DORA, cujo âmbito subjetivo abrange as entidades mais relevantes do setor financeiro (entre outras), dispõe, em particular, sobre a necessidade de se estabelecerem e aplicarem processos de gestão, classificação e comunicação de incidentes relacionados com as TIC e obriga à realização de testes de resiliência operacional digital, sensibilizando as autoridades para a importância da gestão do risco de terceiros (abordado *supra*). Este Regulamento impõe igualmente o respeito por alguns princípios fundamentais e confere às autoridades competentes um conjunto de poderes de fiscalização das entidades terceiras prestadoras de serviços. O Regulamento DORA reconhece, também, a importância da partilha de informações entre autoridades com vista ao reforço da eficácia da supervisão através deste processo de cooperação e partilha.

Este Regulamento é, então, constituído por cinco pilares essenciais: a gestão do risco no domínio das TIC; a notificação às autoridades competentes de incidentes de caráter severo relacionados com as TIC e de ciberameaças significativas; a realização de testes de resiliência operacional digital; a partilha de dados e informações sobre ciberameaças e vulnerabilidades; e a gestão do risco associado às TIC devido a terceiros.

No plano nacional, os diplomas, cujo âmbito de aplicação vai desde a Administração Pública, aos operadores de infraestruturas críticas e aos operadores de serviços essenciais, e se estende ainda aos prestadores de serviços digitais, preveem requisitos de segurança e de notificação de incidentes, consagrando, também, regimes de fiscalização e sanções. Isto porque, conforme ressaltamos acima, e o próprio preâmbulo do DL n.º 65/2021 nota que "O desafio da transição digital, de alcance transversal, e a emergência de novas tecnologias disruptivas, como a inteligência artificial, a realidade virtual e aumentada e a Internet das coisas, sublinham a necessidade de assegurar um nível elevado de segurança das redes e dos sistemas de informação que sustentam o uso destas tecnologias, para que decorra num ambiente de confiança e protegido de ameaças que podem ter efeitos desestabilizadores de considerável alcance na vida em sociedade, especialmente em contextos de crise, que tendem a agravar a exploração de vulnerabilidades por parte de agentes de ameaça com motivações diversas".

Deste modo, estes diplomas e orientações visam, sobretudo, reforçar a gestão dos riscos, operacionais e de segurança, associados às TIC por parte das instituições e autoridades, por forma a definirem estratégias e construírem infraestruturas mais resilientes, que permitam mitigar os riscos inerentes à utilização da tecnologia, cientes dos riscos de responsabilidade, de segurança da informação e de confiança/reputacionais que poderão impactar a sua atividade, o seu bom nome e o sistema financeiro na sua globalidade.

Assim, tornando a revolução digital o sistema financeiro mais vulnerável, não podem conter-se esforços, por parte das instituições e das autoridades, para gerir as vulnerabilidades identificadas ao longo do presente estudo e minimizar os riscos delas decorrentes. Além do notado *supra* a este respeito, destaque-se, em particular, o balanço da implementação do TIBER-PT (o quadro de referência para testes de cibersegurança avançados) apresentado pelo Banco de Portugal, a 3 de outubro de 2022, na terceira reunião plenária do Fórum com a Indústria para a Cibersegurança e Resiliência Operacional (FICRO)[180], bem como a proposta de iniciativa de partilha de informação e cooperação entre instituições com vista ao fortalecimento do setor que o Banco apresentou na mesma sede[181]. Refira-se, ainda, a este respeito, os testes de resiliência operacional digital previstos nos artigos 24.º e seguintes do Regulamento DORA, com o objetivo de avaliar a preparação das entidades financeiras para enfrentar ciberameaças e incidentes de carácter severo relacionados com as TIC. Finalmente, note-se o disposto no artigo 45.º do mesmo Regulamento em matéria de acordos de partilha de informações específicas e sensíveis relativas a ciberataques, que permite a partilha pelas entidades financeiras de tais informações (na medida em que tenha por objetivo a melhoria da resiliência operacional digital das entidades, ocorra no seio de entidades de confiança e seja implementada através de acordos de partilha que protejam a natureza sensível das informações partilhadas, respeitem a confidencialidade comercial, a proteção de dados pessoais e as orientações sobre a política de concorrência), admitindo-se o envolvimento das autoridades públicas em tais acordos.

5 Conclusões

A transformação digital do setor bancário e financeiro trouxe uma mudança profunda para o setor, alterando o paradigma na prestação de serviços financeiros.

Tendo em conta as exigências desta transformação, a União Europeia desenhou, desde cedo, uma estratégia para garantir que os quadros de regulação e de supervisão permitam que as empresas que operam no mercado único beneficiem da inovação financeira, assegurando, ao mesmo tempo, um elevado nível de proteção dos consumidores e investidores e a solidez e integridade do sistema financeiro. A partilha de conhecimento e o espírito de cooperação marcam, também, este domínio e reforçam o valor destes temas para o setor, onde já se dão os primeiros passos na implementação de uma Estratégia Digital Europeia e, inclusive, de uma Plataforma Europeia de *Digital Finance*, lançada a 8 de abril de 2022, numa lógica colaborativa entre indústria e autoridades e num esforço conjunto para a construção de um mercado único de *Digital Finance*.

[180] "Constituído em 2021, o FICRO é uma estrutura consultiva do Banco de Portugal que reúne representantes do setor bancário, do principal prestador de serviços de pagamento nacional e da autoridade nacional de cibersegurança, com o objetivo de reforçar a resiliência operacional do sistema financeiro português.", conforme comunicado do BdP disponível em Banco de Portugal apresentou à indústria financeira proposta de cooperação para a cibersegurança | Banco de Portugal (bportugal.pt).

[181] *Idem.*

No panorama internacional tem, também, existido uma aposta cada vez maior por parte das autoridades na participação em diversos fóruns que dão espaço à discussão, teste e experimentação de algumas evoluções tecnológicas — a este respeito, refira-se o *European Forum for Innovation Facilitators* (EFIF), as *Regulatory Sandboxes* e os *Innovation Hubs*.

A transformação atual vai, porém, além das próprias instituições supervisionadas, obrigando, também, à revisão das metodologias de regulação e supervisão por parte das autoridades competentes, que procuram adaptar-se rapidamente às alterações trazidas pela digitalização do setor financeiro e redefinem as suas formas de atuação. Tal como destacado por Benoît Cœuré, o *Head* do *Innovation Hub* do BIS, os Bancos Centrais deverão ter em consideração "*'what impetus and changes are needed' to make the shift to becoming the 'supervisors of the future'*"[182].

Neste contexto, as autoridades de supervisão têm, cada vez mais, promovido a utilização de ferramentas de *Suptech*, integrando-as nos seus processos. Ainda que esta utilização possa facilitar, simplificar e automatizar os procedimentos de conformidade e de comunicação, e, assim, contribuir para melhorar a atividade de supervisão, gera novos desafios, em particular no que diz respeito ao cumprimento pelas próprias autoridades das garantias procedimentais e de princípios jurídicos fundamentais que as vinculam no exercício de poderes públicos, incluindo no contacto com as entidades supervisionadas e com os cidadãos.

Neste estudo, identificámos, em particular, os desafios e riscos, jurídicos e operacionais, que podem surgir em virtude da adoção e utilização de ferramentas tecnológicas no âmbito do exercício de atribuições de supervisão.

Quanto aos desafios jurídicos, estes passam, em primeiro lugar, pelos riscos relacionados com a recolha de uma grande quantidade de dados sensíveis e a correspondente necessidade de garantir a sua segurança.

Além disso, tanto na esfera das entidades supervisionadas, como das próprias autoridades de supervisão, surgem, em particular, riscos ligados ao *outsourcing*, que deverão ser adequadamente enquadrados, de forma a evitar-se a desresponsabilização relativamente às obrigações impostas, tanto a supervisores, como a supervisionados, pela legislação aplicável.

Do mesmo modo, verifica-se a existência de desafios relativos ao cumprimento das garantias processuais aplicáveis no contexto da adoção de decisões de supervisão, ao nível, quer do Direito da União, quer do Direito nacional. Em particular, as decisões adotadas com recurso a ferramentas tecnológicas, como a inteligência artificial (com os seus complexos algoritmos), poderão trazer desafios ao cumprimento das exigências de fundamentação e transparência próprias dos procedimentos administrativos[183,184].

O recurso a estas ferramentas no processo de tomada de decisão obriga, ainda, a que se tenham em especial atenção os princípios e as normas de Direito Administrativo europeu e nacional. Destaque-se, desde logo, os desafios relacionados com o cumprimento do dever de diligência, no âmbito do princípio da boa administração.

[182] A este respeito, veja-se a entrevista dada por CŒURÉ Benoît para a Central Banking Newsdesk "*Cœuré warns of 'black box' problem for regulators*", em 19 de Agosto de 2020 (disponível em Cœuré warns of 'black box' problem for regulators - Central Banking. Quase ipsis verbis o texto da p. 31 — tentaria introduzir ligeiras alterações, se possível.

[183] Ricardo Pedro, — Inteligência Artificial e Arbitragem de Direito Público: Primeiras Reflexões, *op. cit.*, página 109.

[184] Tendo como base estes desafios, a doutrina tem referido a necessidade de criação de um novo sistema de governança, denominado *Algorithmic Regulation*, como sistema de tomada de decisão (K. Yeung, E M. Lodge — Algorithmic Regulation: A Critical Interrogation, 2019, disponível em Algorithmic Regulation: A Critical Interrogation by Karen Yeung :: SSRN), página 6.

Apesar da constante evolução na criação e desenvolvimento de ferramentas de *Suptech*, analisando o panorama atual, receamos que estas ainda não consigam realizar uma avaliação valorativa quanto ao modo como os casos específicos devem ser tratados e decididos, comparando com a avaliação realizada pelo ser humano. Este último reduto não pode ser eliminado e é fundamental para dar cumprimento ao dever de diligência, além de ser um passo necessário para promover a justificação adequada das decisões, que têm de ser compreensíveis, coerentes e transparentes, à luz dos requisitos formais e materiais aplicáveis no nosso ordenamento jurídico.

Por outro lado, a utilização de ferramentas de *Suptech* para proceder a atos menos complexos, nomeadamente para elaborar e transmitir respostas aos supervisionados e público em geral, também não nos parece isenta de desafios, tendo em conta que a entidade pública permanece sempre responsável pela resposta em causa.

Quanto aos desafios operacionais, estes emergem, sobretudo, de riscos de concentração e ciber-riscos, devendo as autoridades definir estratégias e construir infraestruturas mais resilientes, que permitam mitigar estes riscos inerentes à utilização de ferramentas de *Regtech* e de *Suptech*, cientes dos riscos de responsabilidade, de segurança da informação e reputacionais que poderão impactar a sua atividade, o seu bom nome e o sistema financeiro no seu todo. Deverão, a final, ser utilizadas apenas as ferramentas que se entendam compatíveis com os valores da organização, fazendo-se uma análise de risco prévia a qualquer automatização (no fundo, uma análise do grau de risco em questão *vis à vis* o potencial de utilização da ferramenta).

Em suma, ainda que, atualmente, a utilização de ferramentas de *Regtech* e *Suptech* seja reduzida face ao seu potencial futuro — sendo estas utilizadas apenas como meios auxiliares de decisões humanas, e não (pelo menos, por ora) como verdadeiros substitutos destas —, a realidade é que estes fenómenos tenderão a marcar decisivamente o funcionamento do setor bancário e financeiro do futuro, bem como as atividades de regulação e de supervisão.

Embora as iniciativas regulatórias já estejam a dar os primeiros passos para acompanhar os céleres avanços neste domínio e tentar mitigar os principais riscos subjacentes, é certo que os ordenamentos jurídicos, quer nacional, quer europeu, deixam ainda muitas questões em aberto relativamente ao enquadramento e consequências jurídicas da utilização de ferramentas de *Regtech* e *Suptech*.

O presente estudo procurou, numa lógica panorâmica, contribuir para sistematizar as questões suscitadas pelos fenómenos de *Regtech* e *Suptech,* chamando a atenção, em particular, para os desafios relacionados com a aplicação de princípios e garantias de Direito Administrativo. Embora a situação atual seja marcada por uma utilização ainda relativamente modesta de ferramentas tecnológicas dos tipos descritos, o recurso crescente a essas tecnologias, bem como a progressiva sofisticação e desenvolvimento destas, irá provavelmente transformar segmentos importantes da atividade regulatória e de supervisão, quer na vertente das entidades supervisionadas, quer das autoridades de supervisão.

É fundamental, a nosso ver, que o processo de evolução tecnológica seja acompanhado por uma reflexão e pela construção de soluções, que permitam ir orientando e definindo regras e princípios orientadores da ação dos supervisores e dos supervisionados, de modo a permitir conciliar as alterações de comportamento com o conteúdo de princípios fundamentais que, num Estado de Direito, definem a atuação da Administração Pública.

Poderá, igualmente, ser conveniente refletir sobre se o próprio Direito, e (alguns d)os princípios de Direito Administrativo em especial, devem de alguma forma ser repensados de modo a

poderem adaptar-se à novas realidades descritas no presente estudo. Em todo o caso, este estudo procurou sobretudo destacar a pertinência da aplicação dos atuais princípios gerais do Direito Administrativo aos fenómenos em causa, o que também realça a relevância, a durabilidade e a capacidade de adaptação que revelam. Não é, em qualquer caso, objeto deste estudo a análise da aplicação de ferramentas específicas e suas implicações para as autoridades administrativas, nomeadamente para o Banco de Portugal, nas suas várias atribuições e funções, sem prejuízo de se poder revelar pertinente, no futuro, que se proceda a tal reflexão em estudo subsequente – a própria natureza evolutiva da matéria assim o parece justificar e, porventura, reclamar.

6 Referências

Acórdão do Tribunal de Justiça de 21 de novembro de 1991, Hauptzollamt München-Mitte c. Technische Universität München, processo C-269/90, ECLI:EU:C:1991:438, parágrafo 13.

Agência para a Modernização Administrativa (2022). Guia para uma Inteligência Artificial ética, transparente e responsável na Administração Pública: Autor. Disponível em: Guia para a Inteligência Artificial, Ética, Transparente e Responsável.

Almeida, F. (2023). Inteligência Artificial e Atividade Administrativa: notas breves sobre automatização na emissão de atos administrativos. In Revista de Direito Administrativo (pp. 137-144). Lisboa: AAFDL EDITORA.

Andrade, J. F. de, e M. M. Maia, (2019) Fomentar a *Regtech*: o futuro da regulação financeira. In A. M. Cordeiro, A. P. de Oliveira, e D. P. Duarte, *Fintech Novos estudos sobre tecnologia financeira*. Coimbra: Almedina.

Andrade, J. C. V. de. (2016). *A justiça administrativa*. Coimbra: Almedina.

Antunes, H. S. (2020). *Direito e Inteligência Artificial*, Lisboa: UCP Editora.

Antunes, L. F. (2022). Decisão Automatizada baseada em inteligência artificial: utopia ou distopia? In *Cadernos de Justiça Administrativa*, 152, Braga: Centro de Estudos Judiciários.

The Royal Society. (2019). Explainable AI: the basics. Autor. Disponível em: royalsociety.org.

Azevedo, N. S. de (2020). *SupTech: A potential supervisory tool of European Banking Supervisors*. Disponível em SSRN-id3861890.pdf (sharepoint.com).

BIS (n.d.). *Innovation Hub work on suptech and regtech*. Autor. Disponível em BIS Innovation Hub work on Suptech and Regtech.

Broeders, D., e Prenio, J. (2018). *Innovative technology in financial supervision (suptech) – the experience of early users.* FSI Insights on policy implementation, No 9. Disponível em *Innovative technology in financial supervision (Suptech) - the experience of early users (bis.org).

Castri, S. di, et al. (2019). *The Suptech Generations.* FSI Insights on policy implementation No 19. BIS. Disponível em The suptech generations (bis.org).

Caupers, J., e Eiró, V. (2016). *Introdução ao Direito Administrativo*. 12ª Edição. Ancora Editoras.

Coelho, R. et al. (2019). *Suptech applications for anti-money laundering*. FSI Insights on policy implementation No 18. BIS. Disponível em Suptech applications for anti-money laundering (bis.org).

Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre a revisão intercalar relativa à aplicação da Estratégia para o Mercado Único Digital, de 10 de maio de 2017 (COM(2017) 228 final).

Comunicação da Comissão "Plano de Ação para a Tecnologia Financeira: rumo a um setor financeiro europeu mais competitivo e inovador" (COM(2018) 109 final), de 8 de março de 2018.

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 UE, de 24 de setembro de 2020 (COM(2020) 591 final).

Comunicação da Comissão "Plano de Ação para a Tecnologia Financeira: rumo a um setor financeiro europeu mais competitivo e inovador" (COM(2018) 109 final), de 8 de março de 2018.

Conselho da União Europeia. (2023). *ChatGPT in the Public Sector – overhyped or overlooked?* Autor. Disponível em art-paper-chatgpt-in-the-public-sector-overhyped-or-overlooked-24-april-2023_ext.pdf (europa.eu).

Cœuré, B. (2020). "Cœuré warns of 'black box' problem for regulators". *Central Banking*. Disponível em Cœuré warns of 'black box' problem for regulators - Central Banking.

Elliott, J., e Jenkinson, N. (2020). *Cyber Risk is the New Threat to Financial Stability*. Disponível em Cyber Risk is the New Threat to Financial Stability (imf.org).

Denis, E., e Blume, D. (2021). *Using digital technologies to strengthen shareholder participation*. Going Digital Toolkit Policy Note, No. 9. Disponível em Using digital technologies to strengthen shareholder participation (oecd.org).

EBA (2020). *EBA Report On Big Data And Advanced Analytics*. Paris. Autor. Disponível em Final Report on Big Data and Advanced Analytics.pdf (europa.eu).

ESMA. (2019). *ESMA Report on Trends, Risks and Vulnerabilities, Financial innovation Regtech and Suptech – change for markets and authorities*, No 1. Autor. Disponível em trv_2019_1-Regtech_and_Suptech_change_for_markets_and_authorities.pdf (europa.eu).

FSB. (2022). *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*. Autor. Disponível em: The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions: Market developments and financial stability implications (fsb.org)

Gonçalves, C. (2020). As Big tech como *players* do Sistema Financeiro. Dissertação de Mestrado, ISG. Disponível em https://comum.rcaap.pt/bitstream/10400.26/34109/1/Tese_Carlos_Gon%C3%A7alves_Vers%C3%A3o_Final.pdf).

Gonçalves, P. C. (2019). *Manual de Direito Administrativo*, Volume 1. Coimbra: Almedina.

International Association of Insurance Supervisors. (2019). *Regtech and Suptech: Implications for Supervision*. Eschborn. Disponível em regtech_and_suptech_implications_for_supervisors_consultation_call_report.pdf (a2ii.org).

Internet Society (2017). *Artificial Intelligence and Machine Learning: Policy Paper*, *Internet Society*. Disponível em Artificial Intelligence & Machine Learning: Policy Paper | Internet Society.

OECD. (2021). *OECD Business and Finance Outlook 2021: AI in Business and Finance*. Paris: OECD Publishing. https://doi.org/10.1787/ba682899-en.

I Oliveira, e J. L Dias, (2023). *Inteligência Artificial e Proteção de Dados.* In Pedro, R., e Caliendo, P. (Coord.), *Inteligência Artificial no Contexto do Direito Público: Portugal e Brasil*, 1.ª edição (pp. 145 a 164) Coimbra: Almedina.

Otero, P. (2016). *Direito do Procedimento Administrativo*, Volume I. Coimbra: Almedina.

Paula, A. (2021). *Serão as redes dos serviços financeiros seguras?*, disponível em Os riscos de cibersegurança que os serviços financeiros enfrentam | WatchGuard Blog.

Pedro, R. (2023). Inteligência Artificial e Arbitragem de Direito Público: Primeiras Reflexões. In R. Pedro, e P. Caliendo(Coord.), *Inteligência Artificial no Contexto do Direito Público: Portugal e Brasil*, 1.ª edição (pp. 105 a 128) Coimbra: Almedina.

Serra, A. P. et al. (2022). *Regtech* e *Suptech*. *Infor Banca, Revista do Instituto de Formação Bancária*, n.º 125. Disponível em InforBanca-125-JUN2022.pdf (ifb.pt).

Silva, A. F. da. (2021). Inteligência Artificial e Direito Administrativo. In Silva, A. F. da. (Coord.) *Direito Administrativo e Tecnologia*, 2.ª Edição (pp. 9-28). Coimbra: Almedina.

Toronto Centre. (2018). *SupTech: Leveraging Technology for Better Supervision*. Disponível em SupTech: Leveraging Technology for Better Supervision (torontocentre.org)).

Toronto Centre. (2021). *Using Suptech to improve supervision: Essay Winners 2021*. Disponível em Using_SupTech_to_Improve_Supervision.pdf (torontocentre.org).

Vaz, A. (2007). *Segurança da Informação, Protecção da Privacidade e dos Dados Pessoais*, n.º 117 – 3ª Série. Disponível em nr-117_pdf.PMD (rcaap.pt).

Yeung, K., e Lodge, M. (2019). *Algorithmic Regulation: A Critical Interrogation*. Disponível em Algorithmic Regulation: A Critical Interrogation by Karen Yeung :: SSRN.

Zeranski, S., e Sancak, I. E. (2022). Digitalization of Financial Supervision with Supervisory Technology (Suptech). In *Journal of International Banking Law & Regulation*, 8. Disponível em Digitalisation of Financial Supervision with Supervisory Technology (SupTech) by Stefan Zeranski, Ibrahim E. Sancak :: SSRN.

3 Imunidade de jurisdição, perante os tribunais dos Estados-Membros, dos governadores dos bancos centrais nacionais: anotação ao acórdão do Tribunal de Justiça de 30 de novembro de 2021 (Processo C–3/20, LR Ģenerālprokuratūra)

Isabel Alexandre[185]

Abstract

In its judgment of 30 November 2021 in Case C-3/20, the Court of Justice ruled on the limits on criminal prosecution in the Member States, where acts performed by governors of the national central banks are being investigated.

Although the Court of Justice provides guidance that the investigation is not affected by this circumstance and only the trial can be affected by it – and only if the relevant acts were performed in the context of the duties the governors carry out on behalf of the European Central Bank –, there are several obligations incumbent upon the national authorities in cases where they are aware of the existence of immunity from criminal proceedings.

This analysis highlights the main practical implications of the judgment and a number of issues left unresolved, in particular the specific acts which may be covered by the immunity from criminal proceedings of governors.

[185] Departamento de Serviços Jurídicos do Banco de Portugal.

1 O processo principal e as questões prejudiciais

O acórdão do Tribunal de Justiça (TJ) de 30 de novembro de 2021, ora anotado, foi proferido na sequência de um reenvio a título prejudicial de um tribunal letão, perante o qual pendia um processo penal por corrupção e branqueamento de capitais contra um antigo governador do banco central da Letónia, por factos ocorridos durante o exercício destas funções (entre 21 de dezembro de 2001 e 21 de dezembro de 2019).

No âmbito do referido processo penal levantou-se o problema de saber se o arguido podia ser criminalmente perseguido e julgado por um tribunal da Letónia, atendendo a que, enquanto governador do banco central da Letónia, integrara o Conselho Geral do Banco Central Europeu (BCE) desde a adesão da República da Letónia à União Europeia em 1 de maio de 2004, bem como o Conselho do BCE desde a adesão da República da Letónia à zona euro em 1 de janeiro de 2014, e os membros destes órgãos beneficiam, à luz do direito europeu, de imunidade de jurisdição perante os tribunais nacionais.

Para resolver tal problema, o tribunal letão do reenvio colocou, em síntese, as seguintes questões ao TJ:

1. Se um governador de um banco central de um Estado-Membro beneficia da imunidade de jurisdição atribuída aos funcionários e outros agentes da União pelo artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades (adiante, Protocolo), pois o Protocolo, por força do seu artigo 22.º, é aplicável ao Banco Central Europeu, aos membros dos seus órgãos e ao seu pessoal;

2. Se essa imunidade de jurisdição, caso um governador de um banco central de um Estado-Membro dela beneficie, continua a ser assegurada, num processo penal, após a cessação de funções;

3. Se essa imunidade de jurisdição, caso um governador de um banco central de um Estado-Membro dela beneficie, impede uma ação penal num Estado-Membro contra o mesmo governador ou a utilização das provas recolhidas no respetivo inquérito;

4. Se essa imunidade de jurisdição, caso um governador de um banco central de um Estado-Membro dela beneficie, permite à autoridade nacional competente para o processo penal aferir se os factos praticados pelo governador se relacionam com o exercício das suas funções num órgão do BCE e, só na eventualidade de assim concluir, pedir o levantamento da correspondente imunidade ao BCE;

5. Se a imunidade de jurisdição dos funcionários e outros agentes da União, atribuída pelo artigo 11.º, alínea a), do Protocolo, pode abranger atos não relacionados com as funções que aqueles exercem numa instituição da União, mas com as funções exercidas num Estado-Membro.

2 Síntese da pronúncia do Tribunal de Justiça

À primeira questão prejudicial colocada pelo tribunal letão no processo C–3/20, respondeu o TJ que *o artigo 22.º do Protocolo estende aos governadores dos bancos centrais dos Estados-Membros a imunidade de jurisdição atribuída pelo artigo 11.º, alínea a), do Protocolo aos funcionários e outros agentes da União*.

Para atingir tal conclusão, o TJ começou por observar que o Protocolo é aplicável aos governadores dos bancos centrais dos Estados-Membros por força do seu artigo 22.º: no caso dos governadores dos bancos centrais dos Estados-Membros cuja moeda seja o euro, porque são membros do Conselho do BCE e este é um órgão de decisão do BCE; no caso da generalidade dos governadores dos bancos centrais dos Estados-Membros, porque são membros do Conselho Geral do BCE, e este é também um órgão de decisão do BCE.

Seguidamente, o TJ considerou que o regime da imunidade de jurisdição dos governadores dos bancos centrais dos Estados-Membros não está contido nem nos artigos 8.º e 9.º, nem no artigo 10.º, todos do Protocolo: no primeiro caso, porque aqueles preceitos têm apenas como destinatários os membros do Parlamento Europeu; no segundo caso, porque, por um lado, o artigo 10.º tem em vista os representantes dos Estados-Membros que participam nos trabalhos das instituições da União e os governadores dos bancos centrais dos Estados-Membros não podem solicitar nem receber instruções das autoridades nacionais, e porque, por outro lado, aqueles representantes não beneficiam de imunidade de jurisdição nos próprios Estados que representam.

Por último, entendeu o TJ que, embora os governadores dos bancos centrais dos Estados-Membros tenham uma posição diferente dos funcionários e outros agentes da União mencionados no artigo 11.º, alínea a), do Protocolo (quer por serem nomeados e poderem ser demitidos pelos Estados-Membros, quer por não estarem subordinados a uma instituição da União), as seguintes razões militam no sentido de tal preceito ser aplicável aos governadores: a de também eles atuarem por conta de uma instituição da União (o BCE) quando exercem as funções de membro do Conselho ou do Conselho Geral do BCE; a de também eles deverem beneficiar das imunidades necessárias ao cumprimento da missão do BCE; a de também eles deverem beneficiar das imunidades necessárias ao asseguramento da sua independência perante as autoridades nacionais no interesse da União; a de a inaplicabilidade do artigo 11.º, alínea a), do Protocolo aos governadores ter como paradoxal consequência privar de qualquer imunidade os responsáveis pela condução, livre de qualquer influência, da política monetária da União; a de os membros dos órgãos do BCE não deverem ter uma proteção inferior à do pessoal do BCE, ao qual o artigo 22.º, n.º 1, do Protocolo concede a imunidade de jurisdição de que goza o pessoal das outras instituições da União.

Quanto à segunda questão prejudicial colocada pelo tribunal letão no processo C-3/20, a resposta do TJ foi a de que *os governadores dos bancos centrais dos Estados-Membros continuam a beneficiar da imunidade de jurisdição consagrada no artigo 11.º, alínea a), do Protocolo após a cessação das suas funções*: tal conclusão decorreria da circunstância de este preceito, que (como se viu) lhes é aplicável em virtude do disposto no artigo 22.º do mesmo Protocolo, determinar expressamente a continuação desse benefício.

Em relação à quarta questão prejudicial colocada pelo tribunal letão no processo C-3/20 (de que o TJ tratou antes da terceira), respondeu o TJ no sentido de que *as autoridades nacionais responsáveis pelo processo penal podem verificar se os governadores dos bancos centrais dos Estados-Membros atuaram no exercício das suas funções num órgão do BCE e devem, em caso de dúvida quanto à qualidade em que eles atuaram, solicitar e respeitar o parecer do BCE quanto a este ponto, cabendo ao BCE apreciar, sem prejuízo da eventual fiscalização desta apreciação pelo TJ, os pedidos de levantamento da imunidade de jurisdição dos governadores/membros de órgãos do BCE.*

Aquele poder de verificação das autoridades nacionais justifica-se, segundo o TJ, por dois motivos: o de evitar pedidos de levantamento da imunidade de jurisdição relativamente a quaisquer atos penalmente relevantes que os governadores possam cometer, ainda que

manifestamente fora do âmbito das suas funções num órgão do BCE (como é o caso da corrupção e do branqueamento de capitais) e, como tal, fora dos objetivos que presidem à atribuição dessas imunidades; o de permitir o normal exercício pelos Estados-Membros da sua competência em matéria penal quando os interesses da União não estão em jogo.

Por sua vez, o dever das autoridades nacionais de consultarem o BCE em caso de dúvida sobre se os governadores atuaram no âmbito das suas funções num órgão desta instituição, o de acatarem o parecer que o BCE emita a propósito, bem como o de solicitarem ao BCE o levantamento da imunidade de jurisdição (caso o BCE determine que o ato foi praticado na qualidade oficial e as autoridades nacionais pretendam prosseguir o processo que tem esse ato como objeto) resultam, para o TJ, do princípio da cooperação leal previsto no artigo 4.º, n.º 3, do Tratado da União Europeia e do disposto no artigo 18.º do Protocolo.

Já a competência do BCE para a apreciação do pedido de levantamento da imunidade resulta do artigo 17.º do Protocolo, deste preceito decorrendo também que o pedido deve ser deferido, salvo demonstração de que os interesses da União a tal se opõem.

Finalmente, a competência do TJ para fiscalizar o cumprimento dos assinalados deveres das autoridades nacionais e do BCE exerce-se nos termos gerais previstos nos Tratados: através da ação de incumprimento prevista no artigo 258.º do Tratado sobre o Funcionamento da União Europeia, no caso de aquelas violarem o seu dever de consulta; através do recurso previsto no artigo 263.º do mesmo Tratado, a interpor pelo Estado-Membro no caso de indevida recusa de levantamento da imunidade pelo BCE, e sem prejuízo de a validade desta recusa poder ser também objeto de um pedido prejudicial (nos termos do artigo 267.º desse Tratado); através do recurso previsto no artigo 263.º do mesmo Tratado, a interpor pelo governador/membro do órgão do BCE nos termos dos artigos 90.º, n.º 2, e 91.º do Estatuto dos Funcionários da União Europeia, no caso de indevido levantamento da sua imunidade de jurisdição pelo BCE.

Em relação à terceira questão prejudicial colocada pelo tribunal letão no processo C-3/20, o TJ pronunciou-se no sentido de que *a imunidade de jurisdição atribuída pelo artigo 11.º, alínea a), do Protocolo*, ao traduzir um conceito autónomo do direito da União, que deve ser objeto de uma interpretação uniforme na União, *opõe-se a que os seus beneficiários sejam julgados e condenados por um tribunal nacional, mas não se opõe às medidas de investigação, à obtenção de provas e à notificação do despacho de acusação — sem prejuízo do dever das autoridades nacionais de pedirem o levantamento de tal imunidade ao BCE assim que verifiquem a sua existência —, nem à utilização posterior dos elementos de prova recolhidos durante o inquérito.*

A circunstância de a referida imunidade de jurisdição não impedir medidas de investigação, obtenção de provas ou notificações de despachos de acusação dirigidas aos seus beneficiários resulta, segundo o TJ: da contraposição entre o artigo 11.º, alínea a) e os artigos 8.º e 9.º do Protocolo, pois estes, ao contrário daquele, fazem referência ao procedimento penal; de a apreciação dos requisitos da imunidade consagrada no artigo 11.º, alínea a), do Protocolo (prática do ato na qualidade oficial e necessidade de proteção dos interesses da União) pressupor geralmente investigações policiais ou judiciais e a obtenção de elementos de prova; dos próprios valores estabelecidos no artigo 2.º do Tratado da União Europeia, que rejeitam a isenção de responsabilidade penal e o entrave abusivo ao exercício da justiça penal nos Estados-Membros.

Por outro lado, o dever das autoridades nacionais de pedirem o levantamento da imunidade de jurisdição na fase das investigações, se nesta fase dela se aperceberem, decorre dos (já assinalados) artigos 4.º, n.º 3, do Tratado da União Europeia e 18.º do Protocolo.

No que diz respeito à utilização posterior dos elementos de prova recolhidos durante o inquérito, a imunidade de jurisdição não a impede quando se trate de processos relativos a atos não abrangidos pela imunidade, ou de processos dirigidos contra terceiros, apenas a impedindo quando se trate de julgar ou condenar o seu beneficiário: este circunscrito alcance da imunidade explica-se, segundo o TJ, pela circunstância de a mesma apenas dizer respeito a um específico ato praticado por determinada pessoa.

Por último, e quanto à quinta questão prejudicial, a resposta do TJ foi a de que *os artigos 11.º, alínea a), e 17.º do Protocolo não atribuem aos governadores dos bancos centrais dos Estados-Membros imunidade de jurisdição relativamente a atos que não hajam praticado no exercício das suas funções num órgão do BCE*.

Tal conclusão decorre quer da referência à prática dos atos na qualidade oficial dos seus sujeitos, constante daquele primeiro preceito, quer da menção a um interesse da União, constante do segundo, e implica, segundo o TJ, que a autoridade nacional não deva formular ao BCE pedidos de levantamento da imunidade quando verifique que a infração cometida pelo governador não constitui um ato praticado no âmbito das suas funções em órgão do BCE.

A não abrangência dos atos praticados fora do âmbito das funções num órgão do BCE na referida imunidade de jurisdição dos governadores não significa, porém, para o TJ, que relativamente a tais atos os Estados-Membros possam exercer pressões que conflituem com a independência que o direito europeu exige aos membros dos órgãos de decisão do BCE e aos próprios bancos centrais nacionais, bem como que tais pressões não possam desencadear processos por incumprimento da obrigação de cooperação leal que impende sobre os Estados-Membros.

3 Principais efeitos do acórdão nos processos penais movidos a governadores dos bancos centrais nacionais

1. Considerações gerais

Embora os Tratados não consagrem expressamente o caráter obrigatório, em processos judiciais diversos daquele no qual foi suscitada e resolvida a questão prejudicial, dos acórdãos do TJ que procedem à interpretação do direito europeu nos termos do artigo 267.º do Tratado sobre o Funcionamento da União Europeia[186], é, pelo menos, de aceitar o valor persuasivo de tais acórdãos nesses processos, pelo que o acórdão ora anotado tem natural relevância na generalidade dos processos penais que eventualmente corram nos Estados-Membros por factos praticados por governadores de bancos centrais nacionais.

Não é também de excluir que a doutrina do acórdão valha em processos penais instaurados contra outras pessoas (diversas dos governadores dos bancos centrais nacionais) que exerçam

[186] Sobre esta questão, e referindo que a jurisprudência europeia "consagrou a obrigatoriedade das questões prejudiciais de interpretação para os órgãos jurisdicionais nacionais que julguem a causa (incluindo assim os órgãos de recurso), preconizando a doutrina um efeito vinculativo tendencialmente *erga omnes* das decisões prejudiciais", veja-se Maria José Rangel de Mesquita, *Introdução ao Contencioso da União Europeia: Lições*, 4.ª ed., Coimbra, Almedina, 2022, pp. 180-181. O eventual efeito vinculativo das decisões prejudiciais interpretativas em processos diversos do processo principal distingue-se, em qualquer caso, quer do efeito positivo do caso julgado, quer do precedente próprio dos ordenamentos de *Common Law*, assumindo contornos específicos: quanto a este ponto, e para mais desenvolvimentos, veja-se Szymon Kohlhepp, *Die unionsrechtlich veranlasste Rechtskraftdurchbrechung*, Berlin, Duncker & Humblot, 2022, pp. 77-80.

simultaneamente funções em órgãos de instituições europeias e em entidades de direito interno (como é o caso dos membros das autoridades nacionais competentes que integram as equipas conjuntas de supervisão e as equipas de inspeção no local que agem sob a coordenação do BCE: cf. os artigos 3.º, n.º 1, 4.º, 143.º, n.º 1, e 144.º do Regulamento (UE) n.º 468/2014 do Banco Central Europeu, de 16 de abril de 2014, que estabelece o quadro de cooperação, no âmbito do Mecanismo Único de Supervisão, entre o Banco Central Europeu e as autoridades nacionais competentes e com as autoridades nacionais designadas (Regulamento-Quadro do MUS) (BCE/2014/17)) e relativamente às quais, portanto, possa suscitar-se a dúvida sobre a qualidade em que atuam.

Limitar-nos-emos a assinalar os aspetos tratados no acórdão que, do nosso ponto de vista, assumem maior importância prática.

2. Quanto à competência das autoridades nacionais para a promoção desses processos

O acórdão releva, em primeiro lugar, no aspeto em que não configura a imunidade de jurisdição de que os governadores podem beneficiar (pela circunstância de exercerem funções em órgãos do BCE) como um obstáculo à promoção, contra eles, de processos penais nos Estados-Membros.

Efetivamente, tal imunidade de jurisdição deve ser entendida, à luz de elementos literais e teleológicos, apenas como um *impedimento ao julgamento ou à condenação dos governadores*, mas não já como um impedimento à prática de atos de investigação, de recolha de prova ou de notificação da acusação.

A competência das autoridades nacionais para o exercício da ação penal é, assim, e ao menos nas fases desta ação que antecedem o julgamento, salvaguardada, não devendo tais autoridades entender que a sua atuação está paralisada ou dificultada em virtude de os factos a investigar terem sido praticados por um sujeito que pode não vir a ser julgado, por se chegar à conclusão de que beneficia de uma imunidade de jurisdição.

O não condicionamento das normais competências de investigação das autoridades nacionais resulta também do reconhecimento, pelo TJ, de que *as autoridades nacionais (e não apenas o BCE ou o TJ) podem verificar a existência de uma imunidade de jurisdição*.

Por haver esta relação causal, o TJ tratou da quarta questão prejudicial (que versava sobre esse poder de verificação das autoridades nacionais) antes de tratar da terceira (que versava sobre os atos processuais afetados pela imunidade de jurisdição): é que se as autoridades nacionais, sempre que obtivessem a notícia de um crime praticado por um governador de um banco central, estivessem dependentes de uma pronúncia do BCE acerca da existência ou não de uma imunidade de jurisdição desse governador, não a podendo apreciar por sua iniciativa, seria difícil sustentar a circunscrição de tal imunidade ao julgamento ou à condenação, pois toda a atividade investigatória prévia ficaria paralisada até àquela pronúncia.

O TJ esclareceu, porém, que só em caso de dúvida as autoridades nacionais têm o dever de questionar o BCE sobre a existência da referida imunidade, naturalmente acatando depois o respetivo parecer.

Quando, porém, a investigação penal exija a aplicação de uma medida suscetível de interferir no exercício, pelos governadores, das respetivas funções, manter-se-á esta lata competência das autoridades nacionais?

A resposta a este ponto — aliás não tratado no acórdão sob anotação, porque nenhuma das questões prejudiciais que haviam sido colocadas pelo tribunal de reenvio com ele se prendia — impõe que se recorde os processos apensos C-202/18 e C-238/18, que também correram perante o TJ, mas foram instaurados, respetivamente, pelo governador do banco central da Letónia arguido no processo criminal de que emergiu o acórdão ora anotado, bem como pelo BCE.

Com efeito, neles o TJ anulou, por acórdão de 26 de fevereiro de 2019, uma decisão de uma autoridade letã que proibira aquele governador de exercer as suas funções no banco central da Letónia (por suspeita de tráfico de influências em benefício de um banco letão), com o fundamento de que a República da Letónia não demonstrou que tal demissão assentara na existência de indícios suficientes de que o mesmo governador cometera uma falta grave, na aceção do artigo 14.º-2, segundo parágrafo, dos Estatutos do Sistema Europeu de Bancos Centrais (SEBC) e do BCE, tendo, portanto, tal decisão caráter injustificado.

Ora, embora neste acórdão de 2019 (cf. o seu n.º 91) o TJ tivesse ressalvado que "não cabe ao Tribunal de Justiça, quando chamado a decidir com fundamento no artigo 14.º-2 dos referidos estatutos, substituir os tribunais nacionais competentes para decidir sobre a responsabilidade penal do governador em questão nem sequer interferir no inquérito penal preliminar instruído contra este último pelas autoridades administrativas ou judiciais competentes nos termos do direito do Estado-Membro em causa", bem como que "para as necessidades de tal inquérito, nomeadamente para impedir que o governador em causa lhe faça obstrução, pode ser necessário decidir a suspensão temporária deste último das suas funções" (n.º 91), nele também se fez questão de salientar (cf. o seu n.º 92) que "[e]m contrapartida, incumbe ao Tribunal de Justiça, no âmbito das competências que lhe são conferidas pelo artigo 14.º-2, segundo parágrafo, dos Estatutos do SEBC e do BCE, verificar se uma proibição provisória, imposta ao governador em causa, de exercer as suas funções só é decretada se existirem indícios suficientes de que este cometeu uma falta grave suscetível de justificar tal medida".

Portanto, e em suma, *o acórdão ora anotado não pode ser interpretado no sentido de que todos os atos que precedem o julgamento de um processo penal movido contra um governador de um banco central nacional, porque uma eventual imunidade de jurisdição não os condiciona, são exclusivamente regulados pelos direitos internos dos Estados-Membros, não assumindo relevância no plano do direito europeu*: o citado acórdão de 2019 obsta, na verdade, a tal interpretação.

Por outro lado, o acórdão ora anotado tem a preocupação de salientar que *a salvaguarda da normal competência investigatória das autoridades nacionais não as isenta do cumprimento do dever de cooperação leal com o BCE,* que encontra consagração genérica no artigo 4.º, n.º 3, do Tratado da União Europeia (TUE), *quer pedindo e respeitando o parecer do BCE, se tiverem dúvidas quanto à existência de uma imunidade de jurisdição, quer pedindo-lhe o levantamento dessa imunidade, assim que desta se apercebam.*

O acórdão não é, todavia, claro quanto à questão de saber se as autoridades nacionais podem prosseguir a sua investigação no período que necessariamente mediará entre o pedido formulado ao BCE para dilucidação da dúvida acerca da existência da imunidade e a emissão do correspondente parecer pelo BCE.

Atendendo a que a imunidade de jurisdição do governador é encarada, pelo acórdão, como um limite ao julgamento ou à condenação, mas não à investigação, dir-se-ia que nenhum entrave existe ao prosseguimento da investigação nesse período; mas como, se assim fosse, não se compreenderia a necessidade de formulação imediata do pedido de esclarecimento ao BCE,

parece que, *até à pronúncia do BCE, se justifica uma contenção das autoridades nacionais no que diz respeito aos atos sob investigação que apenas envolvam o governador, pelo menos se a investigação não for urgente*.

O acórdão não é também totalmente claro quanto à questão de saber se, no período que medeia entre o pedido de levantamento da imunidade e a sua decisão, ou após uma eventual recusa do BCE de levantamento da imunidade de jurisdição, a investigação pode prosseguir.

Mais uma vez atendendo a que tal imunidade apenas diz respeito ao julgamento ou à condenação, pareceria ser afirmativa a resposta, isto é, pareceria que a autoridade nacional pode continuar a recolher provas relativas aos atos do governador sob investigação, só não podendo usá-las em juízo contra ele, por não poder julgá-lo: contudo, tal conclusão é infirmada pela referência, no acórdão, à necessidade de a autoridade nacional formular um pedido de levantamento da imunidade do governador se pretender dar seguimento ao processo penal, o que indicia que se tal levantamento for recusado o processo é encerrado (sem prejuízo de as provas recolhidas poderem ser utilizadas para a abertura de um novo processo contra outras pessoas ou por outros atos) e que até à decisão sobre o pedido de levantamento a investigação fica suspensa.

3. Quanto aos atos abrangidos pela imunidade de jurisdição

O acórdão é, em segundo lugar, importante no ponto em que restringe a imunidade de jurisdição dos governadores dos bancos centrais nacionais aos atos por eles praticados na qualidade de membros de órgãos do BCE, o que significa, na perspetiva dos tribunais nacionais, que só quando se esteja perante esta categoria de atos — necessariamente em número reduzido, pois, como o próprio TJ salienta, "a imunidade de jurisdição está, por força do artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades, limitada aos atos praticados pelos funcionários e outros agentes da União, na sua qualidade oficial, e, por conseguinte, apenas cobre uma pequena parte dos atos penalmente repreensíveis que esses funcionários e agentes podem cometer" — o processo penal porventura iniciado deverá ser encerrado sem julgamento.

Teria sido útil, de qualquer modo, que o TJ tivesse avançado algum critério na determinação dos (poucos) atos suscetíveis de recondução àquela categoria: o TJ esclareceu apenas que os atos de corrupção ou de branqueamento de capitais (aqueles que constituíam o objeto do processo principal) não o podem ser, mas este esclarecimento coloca, ele próprio, a dúvida sobre se algum ato penalmente típico praticado por governadores pode estar coberto por uma imunidade de jurisdição e, não o podendo, sobre o objeto possível, então, da imunidade de jurisdição conferida aos governadores por atos por eles praticados no exercício das suas funções em órgãos do BCE.

Com efeito, se um ato penalmente típico não puder, por natureza, ser praticado no âmbito das funções exercidas por conta do BCE, qual o sentido da atribuição de uma imunidade de jurisdição neste específico âmbito? Tratar-se-á de uma imunidade de jurisdição apenas em matérias não penais?

Da leitura do acórdão ressalta, porém, que a imunidade de jurisdição a que o TJ se refere abrange também a matéria penal, pois se assim não fosse seriam, desde logo, espúrias as considerações feitas no acórdão sobre o alcance da imunidade (que é, como se acabou de ver, o de impedir o julgamento ou a condenação, mas não a generalidade dos atos do processo penal que precedem o julgamento): a determinação desse alcance não teria, na verdade, qualquer interesse, se o TJ não tivesse em vista a matéria penal.

Subsiste, em qualquer caso, e como se disse, a dúvida sobre os atos de natureza penal que podem ser abrangidos por uma imunidade de jurisdição: eventualmente, e tomando como referência o Código Penal português na hipótese de um processo penal instaurado em Portugal, poderá sê-lo a violação do sigilo profissional pelo governador (prevista no artigo 195º daquele Código) quanto a factos conhecidos no exercício das suas funções num órgão do BCE, ou a falsificação de documento do BCE (cf. o artigo 256.º do mesmo Código), mas trata-se de meras conjeturas, sem resposta segura no acórdão.

É também algo ambígua a referência feita no acórdão (cf. os seus n.ºs 95 e 96) aos atos que, não obstante não estarem cobertos pela imunidade de jurisdição de que o governador beneficia, não podem ser alvo de "pressões" suscetíveis de comprometer a independência dos membros dos órgãos de decisão do BCE ou dos bancos centrais nacionais.

O sentido exato da referência só se alcança consultando as Conclusões da Advogada-Geral (com as quais, aliás, o acórdão genericamente coincide), mais precisamente o respetivo n.º 138 (para o qual o acórdão expressamente remete), que contém a seguinte firmação: "É certo que esta independência [do BCE, dos bancos centrais nacionais e dos membros dos respetivos órgãos de decisão] pode sofrer entraves por intermédio de inquéritos e de processos penais nacionais, bem como por força da adoção, também a nível nacional, de medidas de coação contra um governador de um banco central, ainda que esses inquéritos, processos e medidas se relacionem com atribuições estritamente nacionais ou até mesmo com assuntos não oficiais. A pressão política que desta forma se pode gerar, ou o puro e simples impedimento físico de atuação da pessoa em causa — por exemplo, no caso da sua detenção —, são aptos a colocar entraves ao cumprimento independente das atribuições, no quadro do SEBC".

Trata-se, no fundo, de uma recordatória do decidido no acórdão do TJ de 26 de fevereiro de 2019, proferido nos processos apensos C–202/18 e C–238/18, ao qual já se aludiu no anterior ponto 2., a propósito dos limites à competência investigatória das autoridades nacionais: sob o ponto de vista do TJ, não é necessário alargar o leque dos atos cobertos pela imunidade de jurisdição e abranger nesta atos praticados fora das funções exercidas por conta do BCE, pois em relação a estes existem outros meios (diversos do da concessão de uma imunidade de jurisdição) para salvaguardar o interesse da União, quando os Estados-Membros os investiguem (designadamente, acrescentaríamos nós, o da ação de anulação da decisão nacional que demita o governador).

4. Quanto à vigência temporal da imunidade de jurisdição

O acórdão sob anotação esclarece que não apenas os governadores em exercício, mas também aqueles que já cessaram funções podem beneficiar de uma imunidade de jurisdição perante os tribunais dos Estados-Membros: o que interessa para este efeito — e constitui a terceira consequência prática que ressalta do acórdão — é que o objeto do processo penal seja um ato praticado na qualidade oficial de membro de um órgão do BCE (Conselho ou Conselho Geral).

Poderia não ser este o regime, se a imunidade de jurisdição dos governadores assentasse, não no artigo 11.º, alínea a), do Protocolo, mas no seu 10.º, que trata das imunidades dos representantes dos Estados-Membros que participam nos trabalhos das instituições da União, na medida em que este preceito não faz referência à continuação do benefício da imunidade após a cessação de funções.

Todavia, e como se viu, o TJ expressamente rejeitou a equiparação dos governadores a tais representantes, questão que não era clara na doutrina[187].

Esta rejeição, se por um lado implica, na comparação com a imunidade de jurisdição dos referidos representantes dos Estados-Membros, um alargamento da vigência temporal da imunidade de jurisdição dos governadores (e também da sua vigência espacial, porquanto aqueles representantes, segundo o TJ, podem ser demandados perante os tribunais dos seus próprios Estados-Membros, enquanto os governadores não o podem ser), significa, por outro lado, uma restrição do objeto possível da imunidade de jurisdição dos governadores: com efeito, da aplicação do artigo 11.º, alínea a), do Protocolo aos governadores resulta que não basta que a ação emerja da participação nos trabalhos do BCE, ou de uma atuação em nome do BCE, exigindo-se, diversamente, que a ação emerja de um ato praticado na qualidade oficial de membro de um órgão do BCE [188].

ANEXO (Excerto do acórdão anotado)

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Grande Secção)

30 de novembro de 2021

[...]

Quanto às questões prejudiciais

Quanto à primeira questão prejudicial

35. Com a sua primeira questão prejudicial, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 22.o do Protocolo Relativo aos Privilégios e Imunidades deve ser interpretado no sentido de que o governador de um banco central de um Estado Membro pode beneficiar da imunidade de jurisdição prevista no artigo 11.o, alínea a), deste protocolo.

36. Em primeiro lugar, há que observar que o governador de um banco central de um Estado-Membro faz parte das pessoas referidas no artigo 22.º do Protocolo Relativo aos Privilégios e Imunidades.

37. Com efeito, o artigo 22.º, n.º 1, do Protocolo Relativo aos Privilégios e Imunidades prevê que este é aplicável ao BCE, aos membros dos seus órgãos e ao seu pessoal, sem prejuízo do disposto no Protocolo Relativo aos Estatutos do SEBC e do BCE.

38. Ora, por um lado, os governadores dos bancos centrais dos Estados-Membros cuja moeda seja o euro são, em aplicação do artigo 283.º, n.º 1, TFUE e do artigo 10.º–1 do Protocolo Relativo aos Estatutos do SEBC e do BCE, membros de direito do Conselho do BCE, que

[187] Demos conta desta questão no nosso artigo sobre "As imunidades de jurisdição da União Europeia perante os tribunais dos Estados-Membros", in *Cadernos Jurídicos do Banco de Portugal*, 2, 2020, pp. 95-119 (pp. 103-104), disponível em https://www.bportugal.pt/publications/banco-de-portugal/all/8556.

[188] *Idem*, p. 104.

constitui um órgão de decisão do BCE, por força do artigo 129.º, n.º 1, TFUE e do artigo 9.º–3 do Protocolo Relativo aos Estatutos do SEBC e do BCE. Por outro lado, o artigo 44.º-2 deste protocolo dispõe que os governadores dos bancos centrais nacionais dos Estados-Membros são membros do Conselho Geral, terceiro órgão de decisão do BCE nos termos do artigo 44.º–1 do referido protocolo.

39. Por conseguinte, enquanto membro de pelo menos um órgão do BCE, o governador de um banco central de um Estado-Membro figura entre as pessoas referidas no artigo 22.º, n.º 1, do Protocolo Relativo aos Privilégios e Imunidades. Consequentemente, este protocolo é-lhe aplicável.

40. Em segundo lugar, coloca-se a questão de saber se o governador de um banco central nacional pode beneficiar da imunidade de jurisdição prevista no artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades.

41. Com efeito, por um lado, o artigo 22.º, n.º 1, do Protocolo Relativo aos Privilégios e Imunidades não especifica quais as disposições do mesmo protocolo que são aplicáveis às pessoas a que se refere. Por outro lado, o referido protocolo atribui imunidades, variáveis pela sua natureza e extensão, a três categorias de pessoas, às quais a ligação do governador de um banco central nacional não é evidente.

42. Em primeiro lugar, as imunidades dos membros do Parlamento Europeu, previstas nos artigos 8.º e 9.º do Protocolo Relativo aos Privilégios e Imunidades, são definidas em termos que visam especificamente as funções destes últimos e não são, portanto, aplicáveis a um governador de um banco central nacional.

43. Em segundo lugar, as imunidades dos representantes dos Estados-Membros que participam nos trabalhos das instituições da União, que são objeto do artigo 10.º do Protocolo Relativo aos Privilégios e Imunidades, também não podem beneficiar um governador de um banco central nacional. Por um lado, este último não pode ser considerado o representante de um Estado-Membro quando exerce as suas funções de membro do Conselho ou do Conselho Geral do BCE. Com efeito, o artigo 130.º TFUE e o artigo 7.º do Protocolo Relativo aos Estatutos do SEBC e do BCE preveem que, no cumprimento das atribuições que lhes são conferidos pelos Tratados, os governadores dos bancos centrais nacionais não podem solicitar nem receber instruções, nomeadamente por parte das autoridades nacionais (v., neste sentido, Acórdão de 26 de fevereiro de 2019, Rimšēvičs e BCE/Letónia, C–202/18 e C–238/18, EU:C:2019:139, n.º 72). Por outro lado, e em qualquer caso, as imunidades dos representantes dos Estados-Membros que participam nos trabalhos das instituições da União são as «imunidades [...] usuais», o que, como indicou a advogada-geral no n.º 56 das suas conclusões, deve ser entendido como uma remissão para as imunidades previstas pela Convenção de Viena sobre Relações Diplomáticas, celebrada em Viena em 18 de abril de 1961. Ora, essas imunidades, que são concedidas aos diplomatas com vista a assegurar o cumprimento eficaz das funções das missões diplomáticas e consulares no Estado de residência, são, por natureza, inoponíveis pelos seus beneficiários aos Estados de que são representantes. Por conseguinte, o governador de um banco central de um Estado-Membro não pode, em caso algum, invocar o benefício das referidas imunidades em relação às autoridades desse Estado-Membro.

44. Em terceiro lugar, embora os funcionários e os outros agentes da União gozem, por força do artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades, da imunidade de jurisdição no que diz respeito aos atos por eles praticados na sua qualidade oficial, incluindo

as suas palavras e escritos, importa observar que os governadores dos bancos centrais nacionais se encontram numa posição diferente destes últimos. Por um lado, enquanto autoridades nacionais, são nomeados e, se for caso disso, demitidos pelos Estados-Membros (Acórdão de 26 de fevereiro de 2019, Rimšēvičs e BCE/Letónia, C–202/18 e C–238/18, EU:C:2019:139, n.º 72). Por outro lado, não estão subordinados a uma instituição da União, uma vez que, por força do artigo 130.º TFUE e do artigo 7.º do Protocolo Relativo aos Estatutos do SEBC e do BCE, não podem solicitar ou receber instruções das instituições, órgãos ou organismos da União, bem como dos Estados-Membros ou de qualquer outro organismo.

45. Todavia, a posição de um governador de um banco central nacional, uma autoridade nacional, é certo, mas que atua no âmbito do SEBC e que, quando é governador de um banco central nacional de um Estado-Membro cuja moeda seja o euro, integra o principal órgão de direção do BCE, é caracterizada por um desdobramento funcional que se traduz por um estatuto híbrido (Acórdão de 26 de fevereiro de 2019, Ilmārs Rimšēvičs e BCE/Letónia, C–202/18 e C–238/18, EU:C:2019:139, n.º 70). Assim, esse governador atua por conta de uma instituição da União, no caso em apreço o BCE, no exercício das suas funções de membro do Conselho. O mesmo se aplica, como decorre do n.º 38 do presente acórdão, a um governador de um banco central nacional de um Estado-Membro cuja moeda não é o euro no exercício das suas funções de membro do Conselho Geral do BCE.

46. A imunidade de que um governador de um banco central beneficia no exercício das suas funções de membro do Conselho do BCE ou de membro do Conselho Geral do BCE decorre, portanto, da exigência de assegurar as suas imunidades necessárias ao cumprimento da sua missão, conforme previstas no artigo 39.º do Protocolo Relativo aos Estatutos do SEBC e do BCE. Por conseguinte, um governador de um banco central deve beneficiar, no exercício dessas funções, dos privilégios e das imunidades necessários ao cumprimento da missão do BCE.

47. Além disso, a concessão aos governadores dos bancos centrais nacionais do benefício da imunidade de jurisdição prevista no artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades, que visa garantir a independência dos seus beneficiários perante as autoridades nacionais no interesse da União, é suscetível de contribuir para a independência que o artigo 130.º TFUE e o artigo 7.º do Protocolo Relativo aos Estatutos do SEBC e do BCE exigem nomeadamente dos referidos governadores no exercício dos poderes e no cumprimento das atribuições que lhes foram conferidas pelos Tratados e pelo Protocolo Relativo aos Estatutos do SEBC e do BCE.

48. Além disso, uma vez que os governadores dos bancos centrais nacionais não podem manifestamente beneficiar de nenhuma das duas outras imunidades previstas pelo Protocolo Relativo aos Privilégios e Imunidades, negar-lhes igualmente o benefício da imunidade de jurisdição estabelecida no artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades tem por consequência paradoxal privar de qualquer imunidade as pessoas a quem os Tratados confiam a responsabilidade de conduzir a política monetária da União e que pretenderam expressamente subtrair de qualquer influência no exercício dessa atribuição.

49. Por último, o artigo 22.º, n.º 1, do Protocolo Relativo aos Privilégios e Imunidades deve ser interpretado no sentido de que concede ao pessoal do BCE, que refere expressamente, a mesma imunidade de jurisdição de que goza o pessoal das outras instituições da União. Ora, não resulta dos Tratados nem do Protocolo Relativo aos Estatutos do SEBC e do BCE que o

legislador da União tenha pretendido conferir aos membros dos órgãos do BCE, e especialmente aos membros do Conselho do BCE, o seu principal órgão de decisão, uma proteção inferior à de todo o pessoal do BCE.

50. À luz das considerações precedentes, há que responder à primeira questão prejudicial que o artigo 22.º do Protocolo Relativo aos Privilégios e Imunidades, lido à luz do artigo 130.º TFUE e do artigo 7.º do Protocolo Relativo aos Estatutos do SEBC e do BCE, deve ser interpretado no sentido de que o governador de um banco central de um Estado-Membro pode beneficiar da imunidade de jurisdição prevista no artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades para os atos que tenha praticado na sua qualidade oficial de membro de um órgão do BCE.

Quanto à segunda questão prejudicial

51. Com a sua segunda questão prejudicial, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades, lido em conjugação com o artigo 22.º deste protocolo, deve ser interpretado no sentido de que o governador de um banco central de um Estado-Membro continua a beneficiar da imunidade de jurisdição prevista no artigo 11.º, alínea a), do referido protocolo após ter deixado de exercer as suas funções.

52. Em conformidade com esta disposição, os funcionários e os outros agentes da União continuam a gozar da imunidade de jurisdição após a cessação das suas funções. Ora, como se concluiu no n.º 50 do presente acórdão, o governador de um banco central nacional beneficia dessa imunidade de jurisdição enquanto membro de um órgão do BCE, nos termos do artigo 22.º do Protocolo Relativo aos Privilégios e Imunidades. Por conseguinte, mantém o benefício da mesma após ter deixado de exercer as funções de membro desse órgão.

53. Por conseguinte, a cessação das funções de governador de um banco central nacional, que põe termo, nos termos do artigo 10.º-1 do Protocolo Relativo aos Estatutos do SEBC e do BCE, ao exercício de pleno direito das funções de membro de um órgão do BCE por parte deste governador, não retira a este último o benefício da imunidade de jurisdição prevista no artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades.

54. Consequentemente, há que responder à segunda questão prejudicial que o artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades, lido em conjugação com o artigo 22.º do mesmo protocolo, deve ser interpretado no sentido de que o governador de um banco central de um Estado-Membro continua a beneficiar, quanto aos atos praticados na sua qualidade oficial, da imunidade de jurisdição prevista no artigo 11.º, alínea a), do referido protocolo após ter deixado de exercer as suas funções.

Quanto à quarta questão prejudicial

55. Com a sua quarta questão prejudicial, que há que examinar antes da terceira questão, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades, lido em conjugação com o artigo 17.º do mesmo protocolo, deve ser interpretado no sentido de que permite à autoridade nacional responsável pelo processo penal, a saber, segundo a fase do processo, a autoridade encarregada do exercício da ação penal ou o órgão jurisdicional penal competente, declarar,

ela própria, que estão preenchidas as condições da imunidade de jurisdição antes de solicitar o levantamento dessa imunidade à instituição da União em causa.

56. Antes de mais, há que salientar que o artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades dispõe que os funcionários e os outros agentes da União só gozam de imunidade de jurisdição relativamente aos atos por eles praticados «na sua qualidade oficial», isto é, no âmbito da missão confiada à União (Acórdão de 11 de julho de 1968, Sayag e Leduc, 5/68, EU:C:1968:42, p. 585).

57. Além disso, os privilégios e imunidades reconhecidos à União por esse protocolo revestem natureza funcional, uma vez que visam evitar entraves ao funcionamento e à independência da União, o que implica, em particular, que os privilégios, imunidades e facilidades concedidos aos funcionários e outros agentes da União o são exclusivamente no interesse da União (Despacho de 13 de julho de 1990, Zwartveld e o., C-2/88-IMM, EU:C:1990:315, n.os 19 e 20, e Acórdão de 18 de junho de 2020, Comissão/RQ, C-831/18 P, EU:C:2020:481, n.º 47).

58. A fim de garantir essa natureza funcional, o artigo 17.º, primeiro parágrafo, do referido protocolo estabelece que a imunidade é concedida aos funcionários e aos outros agentes da União exclusivamente no interesse da União. O artigo 17.º, segundo parágrafo, do mesmo protocolo aplica o mesmo princípio ao prever que cada instituição da União Europeia deve levantar a imunidade concedida a um funcionário ou a outro agente sempre que considere que o levantamento da imunidade não é contrário aos interesses da União.

59. Decorre do que precede que cabe à instituição da União em causa e não à autoridade nacional responsável pelo processo penal avaliar se o levantamento da imunidade é contrário aos interesses da União.

60. Em contrapartida, nem o artigo 11.º, alínea a), nem o artigo 17.º do Protocolo Relativo aos Privilégios e Imunidades indicam qual é a autoridade competente para apreciar o requisito de aplicação da imunidade de jurisdição recordada no n.º 56 do presente acórdão, a saber, que o ato imputado ao funcionário ou ao agente da União deve ter sido praticado por este último na sua qualidade oficial.

61. Por conseguinte, é à luz do contexto e da finalidade destas disposições do Protocolo Relativo aos Privilégios e Imunidades que deve ser determinada a autoridade competente para apreciar se esse requisito está preenchido.

62. Em primeiro lugar, é a instituição da União a que pertence o funcionário ou o agente implicado que está em melhor posição para determinar em que qualidade este agiu. É mesmo possível que tenha os documentos necessários à declaração da infração (Despacho de 13 de julho de 1990, Zwartveld e o., C–2/88–IMM, EU:C:1990:315). Além disso, a competência que o artigo 17.º, segundo parágrafo, do Protocolo Relativo aos Privilégios e Imunidades confere expressamente à instituição da União em causa de verificar que o pedido de levantamento da imunidade que lhe é dirigido não é contrário aos interesses da União atribui-lhe desse modo competência para se certificar de que o ato imputado ao funcionário ou ao agente foi cumprido na sua qualidade oficial por conta da União. Com efeito, se os atos do funcionário ou do agente não foram cumpridos na sua qualidade oficial, os processos instaurados contra estes últimos são, *a fortiori*, insuscetíveis de lesar os interesses da União. Resulta do que precede que a instituição da União a que pertence o interessado é competente para apreciar a condição recordada no n.º 56 do presente acórdão.

63. Em segundo lugar, tal conclusão não implica, no entanto, que a instituição da União em causa seja, em todas as circunstâncias, competente para apreciar se o ato imputado ao funcionário ou ao agente da União foi por ele cumprido na sua qualidade oficial.

64. Com efeito, como expôs, em substância, a advogada-geral no n.º 93 das suas conclusões, na prática, são as autoridades ou os tribunais competentes dos Estados-Membros que, inicialmente, são confrontados com a questão de saber se existe um obstáculo ao exercício da ação penal contra um membro do pessoal da União devido à imunidade que este último pode invocar, uma vez que apenas eles possuem as informações que permitem determinar se o ato imputado apresenta as características de um ato praticado por esse membro do pessoal na sua qualidade oficial em nome da instituição da União a que pertence.

65. Se, nestas condições, não dispusessem de competência para apreciar se o ato foi praticado na qualidade oficial, seriam obrigadas a pedir à instituição da União em causa o levantamento da imunidade em todos os casos em que o ato impugnado tivesse sido cometido por um funcionário ou um agente da União.

66. No entanto, tal interpretação violaria os objetivos prosseguidos pelos autores dos Tratados ao conferir aos funcionários e outros agentes da União uma imunidade de jurisdição.

67. Com efeito, por um lado, a imunidade de jurisdição está, por força do artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades, limitada aos atos praticados pelos funcionários e outros agentes da União, na sua qualidade oficial, e, por conseguinte, apenas cobre uma pequena parte dos atos penalmente repreensíveis que esses funcionários e agentes podem cometer. A este respeito, resulta da jurisprudência que só estão abrangidos por este conceito os atos que, pela sua própria natureza, devam ser considerados como participação daquele que invoca a imunidade na execução das atribuições da instituição à qual pertence (Acórdão de 11 de julho de 1968, Sayag e Leduc, 5/68, EU:C:1968:42, p. 585). À luz dessa mesma definição, os atos de fraude ou, como no âmbito do litígio no processo principal, de corrupção e branqueamento de capitais estão, por definição, fora do âmbito das funções de um funcionário ou outro agente da União, bem como das funções de um governador de um banco central de um Estado-Membro que integre um órgão do BCE, não podendo, por conseguinte, ser abrangidos pelos atos praticados por essas pessoas na sua qualidade oficial.

68. Por outro lado, resulta do artigo 17.º, primeiro parágrafo, do Protocolo Relativo aos Privilégios e Imunidades que a imunidade de jurisdição visa exclusivamente, evitando que o funcionamento e a independência da União sejam entravados (Despacho de 13 de julho de 1990, Zwartveld e o., C–2/88–IMM, EU:C:1990:315, n.º 19), assegurar a proteção dos interesses da União e não pode, portanto, obstar ao exercício pelos Estados-Membros da sua competência em matéria de repressão das infrações penais quando esses interesses não estão em jogo.

69. Ora, o exercício desta competência estaria comprometido ou, pelo menos, sistematicamente atrasado se a autoridade nacional responsável pelo processo penal estivesse, em todos os casos, obrigada a pedir à instituição da União em causa o levantamento da imunidade logo que seja instaurado um processo penal contra um dos funcionários ou agentes dessa instituição.

70. Por conseguinte, esta autoridade nacional deve poder declarar que a infração cometida por um funcionário ou outro agente da União não foi manifestamente cometida por este no exercício das suas funções.

71. A partilha de competência entre a autoridade nacional responsável pelo processo penal e a instituição da União em causa para apreciar se o ato suscetível de ser objeto de qualificação penal foi realizado por um funcionário ou outro agente da União no exercício das suas funções é, aliás, conforme com a intenção expressa pelos autores dos Tratados no artigo 18.º do Protocolo Relativo aos Privilégios e Imunidades. Com efeito, este artigo prevê que, para efeitos da aplicação do referido protocolo, as instituições da União cooperarão com as autoridades responsáveis dos Estados-Membros interessados.

72. A este respeito, o Tribunal de Justiça declarou que o facto de participar ativamente nos processos judiciais, transmitindo ao juiz nacional documentos e autorizando os seus funcionários ou agentes a serem inquiridos na qualidade de testemunhas no processo nacional constitui uma obrigação para todas as instituições da União, continuando essas instituições, na aplicação do referido protocolo, sujeitas à obrigação de cooperação leal com as autoridades nacionais, nomeadamente judiciais, que lhes incumbe (v., neste sentido, Despacho de 13 de julho de 1990, Zwartveld e o., C–2/88–IMM, EU:C:1990:315, n.ºs 21 e 22)

73. No que respeita às modalidades dessa cooperação, há que salientar que, na prática, a questão de saber se o ato impugnado foi praticado pelo funcionário ou agente da União na sua qualidade oficial se coloca em primeiro lugar à autoridade nacional responsável pelo processo penal e que esta só está em condições de fazer uma apreciação sumária sobre a realidade desse critério. Assim, quando esta última constata que o ato que é objeto do processo penal não foi manifestamente praticado pelo funcionário ou agente da União implicado na sua qualidade oficial, o procedimento relativamente a este pode ser prosseguido dado que não se aplica a imunidade de jurisdição. Em contrapartida, quando, numa qualquer fase do processo penal, a referida autoridade nacional se interroga sobre este ponto, incumbe-lhe, por força do princípio da cooperação leal previsto no artigo 4.º, n.º 3, TUE, e em conformidade com o artigo 18.º do Protocolo Relativo aos Privilégios e Imunidades, consultar a instituição da União em causa e, no caso de esta considerar que o ato foi praticado na qualidade oficial, solicitar-lhe o levantamento da imunidade do funcionário ou do agente em causa.

74. No caso de a autoridade nacional responsável pelo processo penal considerar desde logo que o ato foi praticado pelo funcionário ou agente em causa na sua qualidade oficial, deve dirigir diretamente à instituição da União em causa um pedido de levantamento da imunidade deste se pretender dar seguimento a esse processo. Em conformidade com a regra estabelecida no artigo 17.º, segundo parágrafo, do Protocolo Relativo aos Privilégios e Imunidades, que constitui uma expressão específica da obrigação de cooperação leal que incumbe às instituições, aos órgãos e aos organismos da União para com os Estados-Membros, este pedido de levantamento da imunidade deve ser deferido, salvo se se demonstrar que os interesses da União se opõem a tal. Esse caráter funcional e, deste modo, relativo dos privilégios e imunidades da União, que o Tribunal de Justiça já teve ocasião de sublinhar (Despacho de 13 de julho de 1990, Zwartveld e o., C–2/88–IMM, EU:C:1990:315, n.º 20), impõe-se tanto mais que a eficácia dos processos, nomeadamente penais, nos Estados-Membros é, ela própria, suscetível de ser diretamente abrangida pelos interesses da União, em especial no que respeita à proteção dos interesses financeiros desta (v., neste sentido, Acórdãos de 2 de maio de 2018, Scialdone, C–574/15, EU:C:2018:295, n.ºs 27 a 29; de 5 de junho de 2018, Kolev e o., C–612/15, EU:C:2018:392, n.ºs 53 a 55, e de 18 de maio de 2021, Asociaţia «Forumul Judecătorilor din România» e o., C-83/19, C-127/19, C-195/19, C–291/19, C–355/19 e C–397/19, EU:C:2021:393, n.ºs 212 a 214).

75. O respeito pela repartição e pelo bom exercício das competências acima descritas é assegurado, se for caso disso, pelo Tribunal de Justiça da União Europeia, de acordo com as vias jurídicas previstas nos Tratados. Assim, o incumprimento por parte das autoridades nacionais, incluindo judiciais, responsáveis pelo processo penal, da sua obrigação, decorrente do princípio da cooperação leal, de consultar a instituição da União em causa quando não possam ser razoavelmente excluídas quaisquer dúvidas sobre o facto de o ato constitutivo da suposta infração ter sido praticado na qualidade oficial, pode ser submetido ao Tribunal de Justiça no âmbito do processo por incumprimento previsto no artigo 258.º TFUE. Inversamente, quando o levantamento da imunidade tenha sido pedido à instituição da União em causa e tenha sido recusado por esta, a validade dessa recusa pode ser objeto de uma questão prejudicial do órgão jurisdicional nacional competente ou mesmo de um recurso direto do Estado-Membro em causa com fundamento no artigo 263.º TFUE. Por último, o funcionário ou agente da União em causa pode interpor recurso no Tribunal de Justiça da decisão da instituição da União a que pertence de levantar a sua imunidade de jurisdição nos termos do artigo 90.º, n.º 2, e do artigo 91.º do Estatuto dos Funcionários, por esta decisão constituir um ato lesivo dos seus interesses (Acórdão de 18 de junho de 2020, Comissão/RQ, C–831/18 P, EU:C:2020:481, n.º 48).

76. Tendo em conta a conclusão a que se chegou no n.º 50 do presente acórdão, segundo a qual o governador de um banco central nacional beneficia da imunidade de jurisdição ao abrigo do artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades, enquanto membro de um órgão do BCE nos termos do artigo 22.º deste protocolo, a interpretação que figura nos n.ºs 56 a 75 do presente acórdão aplica-se igualmente ao caso desse governador.

77. À luz das considerações precedentes, há que responder à quarta questão prejudicial que o artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades, lido em conjugação com os artigos 17.º e 22.º do mesmo protocolo, deve ser interpretado no sentido de que a autoridade nacional responsável pelo processo penal, a saber, segundo a fase do processo, a autoridade encarregada do exercício da ação penal ou o órgão jurisdicional penal competente, é competente para apreciar em primeiro lugar se a eventual infração cometida pelo governador de um banco central nacional, na qualidade de membro de um órgão do BCE, resulta de um ato praticado por esse governador no exercício das suas funções nesse órgão, mas é obrigada, em caso de dúvida, a solicitar o parecer do BCE, de acordo com o princípio da cooperação leal, e a respeitar esse parecer. Em contrapartida, cabe exclusivamente ao BCE apreciar, quando lhe é submetido um pedido de levantamento da imunidade desse governador, se esse levantamento de imunidade é contrário aos interesses da União, sob reserva da eventual fiscalização dessa apreciação pelo Tribunal de Justiça.

Quanto à terceira questão prejudicial

78. Com a sua terceira questão prejudicial, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades deve ser interpretado no sentido de que a imunidade de jurisdição nele prevista se opõe a todos os procedimentos criminais, nomeadamente às medidas de investigação, à obtenção de provas e à notificação do despacho de acusação, ou obsta apenas a que os seus beneficiários sejam julgados e condenados por um órgão jurisdicional, e se a referida imunidade de jurisdição obsta à utilização posterior dos elementos de prova recolhidos durante o inquérito.

79. Há que recordar que, segundo jurisprudência constante do Tribunal de Justiça, decorre das exigências tanto da aplicação uniforme do direito da União como do princípio da igualdade

que os termos de uma disposição do direito da União, que não comporte uma remissão expressa para o direito dos Estados-Membros para determinar o seu sentido e o seu alcance, devem normalmente ser objeto, em toda a União, de uma interpretação autónoma e uniforme, independentemente das qualificações utilizadas nos Estados-Membros, tendo em conta os termos da disposição em causa, bem como o seu contexto e os objetivos prosseguidos pela regulamentação de que faz parte [Acórdão de 9 de setembro de 2021, Bundesamt für Fremdenwesen und Asyl (Pedido subsequente de proteção internacional), C–18/20, EU:C:2021:710, n.º 32].

80. Daqui resulta que, na falta de remissão, no artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades, para o direito nacional, o conceito de «imunidade de jurisdição» que consta desta disposição deve ser considerado um conceito autónomo do direito da União cujo sentido e alcance devem ser idênticos em todos os Estados-Membros. Por conseguinte, cabe ao Tribunal de Justiça dar a este conceito uma interpretação uniforme na ordem jurídica da União.

81. No que respeita à redação do artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades, importa salientar que, em todas as versões linguísticas, a imunidade prevista nesta disposição se opõe pelo menos a que os seus beneficiários sejam julgados e condenados por um órgão jurisdicional. Em contrapartida, não se pode deduzir apenas da redação da referida disposição que esta imunidade não abrange igualmente alguns dos atos processuais penais referidos no n.º 78 do presente acórdão, como salienta, em substância, a advogada-geral no n.º 71 das suas conclusões.

82. Por conseguinte, há que interpretar o conceito de «imunidade de jurisdição», na aceção desta disposição, à luz do contexto e dos objetivos prosseguidos por esta última.

83. No que respeita ao contexto do artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades, importa salientar que os artigos 8.º e 9.º deste protocolo definem o alcance da imunidade dos membros do Parlamento Europeu de modo mais preciso do que o dos funcionários e dos outros agentes da União. Resulta destes artigos que a imunidade dos membros do Parlamento é definida como incluindo o procedimento penal e, por conseguinte, não está limitada apenas à fase do julgamento (v., neste sentido, Acórdãos de 21 de outubro de 2008, Marra, C–200/07 e C–201/07, EU:C:2008:579, n.º 27, e de 17 de setembro de 2020, Troszczynski/Parlamento, C–12/19 P, EU:C:2020:725, n.º 39). Em contrapartida, não existe tal precisão no artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades relativamente à imunidade de jurisdição.

84. No que respeita aos objetivos prosseguidos pelo artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades, este último só visa impedir o exercício de ações contra um funcionário ou um agente da União pelas autoridades de um Estado-Membro nos casos excecionais em que o ato que lhe é imputado é praticado pelo referido funcionário ou agente na sua qualidade oficial e na medida estritamente necessária à proteção dos interesses da União. Ora, a apreciação destes requisitos de aplicação da imunidade de jurisdição pressupõe, antes de mais, a demonstração da realidade e da imputabilidade dos factos, tornando assim a maior parte das vezes necessária a realização de uma investigação policial ou judiciária e a obtenção de elementos de prova. Seria, portanto, contrário ao alcance deliberadamente relativo que os autores do Protocolo Relativo aos Privilégios e Imunidades conferiram à imunidade de jurisdição que esta impedisse as investigações policiais ou judiciais.

85. Além disso, uma interpretação demasiado ampla da imunidade de jurisdição, incluindo a investigação policial e judicial e o processo penal preliminar, poderia conferir aos funcionários e aos agentes da União uma quase isenção de responsabilidade penal e entravar abusivamente o exercício da justiça penal no Estado-Membro em questão quando um deles estivesse envolvido, o que seria contrário aos valores, estabelecidos no artigo 2.º do TUE, a que os autores dos Tratados aderiram, e em particular ao Estado de direito. A este respeito, não se justifica, nomeadamente, que a autoridade responsável pelo processo penal não o possa notificar de um despacho de acusação.

86. Resulta do exposto que a imunidade de jurisdição prevista no artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades não se opõe aos processos penais no seu conjunto, nomeadamente às medidas de investigação, à obtenção de provas e à notificação do despacho de acusação.

87. No entanto, se, logo na fase das investigações conduzidas pelas autoridades nacionais e antes de recorrer a um órgão jurisdicional, se constatar que o funcionário ou agente da União pode beneficiar da imunidade de jurisdição relativamente aos atos que são objeto de procedimento penal, cabe a essas autoridades, em conformidade com o artigo 4.º, n.º 3, TUE e com o artigo 18.º do Protocolo Relativo aos Privilégios e Imunidades, pedir o levantamento da imunidade à instituição da União em causa, a qual está então obrigada a agir, em particular, em conformidade com o exposto nos n.ºs 58, 62 e 74 do presente acórdão.

88. No que respeita à questão de saber se a imunidade de jurisdição obsta à utilização posterior dos elementos de prova recolhidos durante o inquérito, resulta do exposto que esta imunidade não tem tal alcance. Esta opõe-se apenas a qualquer utilização das provas recolhidas com o objetivo de julgar e condenar o funcionário ou o agente da União em causa pelo ato abrangido por essa imunidade. Em contrapartida, uma vez que a referida imunidade beneficia apenas o funcionário ou o agente da União em causa para um determinado ato, a mesma não se opõe a que essas provas possam ser utilizadas noutros processos relativos a outros atos não abrangidos pela imunidade ou dirigidos contra terceiros.

89. Pelos mesmos motivos que os referidos no n.º 76 do presente acórdão, a interpretação exposta nos n.ºs 81 a 88 deste último é igualmente pertinente para a apreciação da imunidade de jurisdição de um governador de um banco central de um Estado-Membro, na sua qualidade de membro de um órgão do BCE.

90. À luz das considerações precedentes, há que responder à terceira questão prejudicial que o artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades deve ser interpretado no sentido de que a imunidade de jurisdição que prevê não se opõe aos procedimentos penais no seu conjunto, nomeadamente às medidas de investigação, à obtenção de provas e à notificação do despacho de acusação. No entanto, se, logo na fase das investigações conduzidas pelas autoridades nacionais e antes de recorrer a um órgão jurisdicional, se verificar que a pessoa objeto das investigações é suscetível de beneficiar da imunidade de jurisdição relativamente aos atos que são objeto de procedimento penal, cabe a essas autoridades pedir o levantamento da imunidade à instituição da União em causa. Esta imunidade não se opõe a que os elementos de prova recolhidos durante a investigação possam ser utilizados noutros processos judiciais.

Quanto à quinta questão prejudicial

91. Com a sua quinta questão prejudicial, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 11.º, alínea a), e o artigo 17.º do Protocolo Relativo aos Privilégios e

Imunidades devem ser interpretados no sentido de que a imunidade de jurisdição pode ser oposta no interesse da União quando o beneficiário dessa imunidade é posto em causa no âmbito de um processo penal por atos não relacionados com as funções que exerce por conta de uma instituição da União.

92. Antes de mais, importa recordar que resulta, por um lado, do artigo 11.º, alínea a), do Protocolo Relativo aos Privilégios e Imunidades que os funcionários e os outros agentes da União só gozam de imunidade de jurisdição relativamente aos atos praticados na sua qualidade oficial e, por outro, do artigo 17.º, primeiro parágrafo, desse protocolo que esta imunidade só é concedida se for justificada por um interesse da União.

93. Como foi exposto no n.º 73 do presente acórdão, quando a autoridade responsável pelo processo penal declara que a infração cometida pelo funcionário ou agente da União não constitui manifestamente um ato praticado na sua qualidade oficial, pode excluir a imunidade de jurisdição sem que deva ser apreciada a existência de um interesse da União pela instituição da União em causa no âmbito de um pedido de levantamento da imunidade.

94. Por conseguinte, a imunidade de jurisdição não é aplicável no âmbito de um processo penal instaurado contra um funcionário ou um agente da União relativamente a atos desprovidos de uma ligação com o exercício das suas funções. Como foi recordado no n.º 76 do presente acórdão, esta conclusão é igualmente válida para o governador de um banco central de um Estado-Membro na sua qualidade de membro de um órgão do BCE.

95. A proteção assim concedida pelo Protocolo Relativo aos Privilégios e Imunidades aos beneficiários da imunidade de jurisdição tem, como foi recordado no n.º 74 do presente acórdão, caráter funcional e, portanto, relativo e não permite, nomeadamente, protegê-los, se for caso disso, de eventuais pressões que possam ser intencionalmente exercidas sobre eles através de procedimentos abusivos por atos que não são praticados pelos funcionários ou outros agentes da União na sua qualidade oficial. Todavia, há que recordar que, por força do princípio da cooperação leal, os Estados-Membros estão obrigados, nos termos do artigo 4.º, n.º 3, terceiro parágrafo, TUE, a ajudar a União no cumprimento da sua missão e a abster-se de qualquer medida suscetível de pôr em perigo a realização dos objetivos da União. Ora, tais pressões seriam, como salientou a advogada-geral, em substância, no n.º 138 das suas conclusões, suscetíveis de pôr em causa o funcionamento das instituições da União e, portanto, de pôr em perigo a realização dos objetivos desta.

96. Em qualquer caso, o cumprimento da obrigação de cooperação leal nos termos do artigo 18.º do Protocolo Relativo aos Privilégios e Imunidades e do artigo 4.º, n.º 3, TUE pode ser imposto através de um processo por incumprimento [v. Acórdão de 17 de dezembro de 2020, Comissão/Eslovénia (Arquivos do BCE), C–316/19, EU:C:2020:1030]. Além disso, tratando-se de um governador de um banco central nacional que integra o Conselho do BCE, o artigo 130.º TFUE, reproduzido no artigo 7.º do Protocolo Relativo aos Estatutos do SEBC e do BCE, que garante a independência dos membros dos órgãos de decisão do BCE ou dos bancos centrais nacionais no cumprimento das atribuições e deveres que lhes foram conferidos pelos Tratados e pelo Protocolo Relativo aos Estatutos do SEBC e do BCE, proporcionaria igualmente uma base jurídica adequada à Comissão para que, se for caso disso, o Tribunal de Justiça concluísse que houve manobras destinadas a comprometer esta independência.

97. À luz das considerações precedentes, há que responder à quinta questão prejudicial que o artigo 11.º, alínea a), e o artigo 17.º do Protocolo Relativo aos Privilégios e Imunidades devem

ser interpretados no sentido de que a imunidade de jurisdição não se aplica quando o beneficiário dessa imunidade é posto em causa num processo penal por atos que não foram praticados no âmbito das funções que exerce por conta de uma instituição da União.

[...]

Pelos fundamentos expostos, o Tribunal de Justiça (Grande Secção) declara:

1. O artigo 22.º do Protocolo (n.º 7) Relativo aos Privilégios e Imunidades da União Europeia, lido à luz do artigo 130.º TFUE e do artigo 7.º do Protocolo (n.º 4) Relativo aos Estatutos do Sistema Europeu de Bancos Centrais e do Banco Central Europeu, deve ser interpretado no sentido de que o governador de um banco central de um Estado-Membro pode beneficiar da imunidade de jurisdição prevista no artigo 11.º, alínea a), do Protocolo (n.º 7) Relativo aos Privilégios e Imunidades da União Europeia para os atos que tenha praticado na sua qualidade oficial de membro de um órgão do Banco Central Europeu.

2. O artigo 11.º, alínea a), do Protocolo (n.º 7) Relativo aos Privilégios e Imunidades da União Europeia, lido em conjugação com o artigo 22.º do mesmo protocolo, deve ser interpretado no sentido de que o governador de um banco central de um Estado-Membro continua a beneficiar, quanto aos atos praticados na sua qualidade oficial, da imunidade de jurisdição prevista no artigo 11.º, alínea a), do referido protocolo após ter deixado de exercer as suas funções.

3. O artigo 11.º, alínea a), do Protocolo (n.º 7) Relativo aos Privilégios e Imunidades da União Europeia, lido em conjugação com os artigos 17.º e 22.º do mesmo protocolo, deve ser interpretado no sentido de que a autoridade nacional responsável pelo processo penal, a saber, segundo a fase do processo, a autoridade encarregada do exercício da ação penal ou o órgão jurisdicional penal competente, é competente para apreciar em primeiro lugar se a eventual infração cometida pelo governador de um banco central nacional, na qualidade de membro de um órgão do Banco Central Europeu, resulta de um ato praticado por esse governador no exercício das suas funções nesse órgão, mas é obrigada, em caso de dúvida, a solicitar o parecer do Banco Central Europeu, de acordo com o princípio da cooperação leal, e a respeitar esse parecer. Em contrapartida, cabe exclusivamente ao Banco Central Europeu apreciar, quando lhe é submetido um pedido de levantamento da imunidade desse governador, se esse levantamento de imunidade é contrário aos interesses da União Europeia, sob reserva da eventual fiscalização dessa apreciação pelo Tribunal de Justiça.

4. O artigo 11.º, alínea a), do Protocolo (n.º 7) Relativo aos Privilégios e Imunidades da União Europeia deve ser interpretado no sentido de que a imunidade de jurisdição que prevê não se opõe aos procedimentos penais no seu conjunto, nomeadamente às medidas de investigação, à obtenção de provas e à notificação do despacho de acusação. No entanto, se, logo na fase das investigações conduzidas pelas autoridades nacionais e antes de recorrer a um órgão jurisdicional, se verificar que a pessoa objeto das investigações é suscetível de beneficiar da imunidade de jurisdição relativamente aos atos que são objeto de procedimento penal, cabe a essas autoridades pedir o levantamento da imunidade à instituição da União Europeia em causa. Esta imunidade não se opõe a que os elementos de prova recolhidos durante a investigação possam ser utilizados noutros processos judiciais.

5. O artigo 11.º, alínea a), e o artigo 17.º do Protocolo (n.º 7) Relativo aos Privilégios e Imunidades da União Europeia devem ser interpretados no sentido de que a imunidade de jurisdição não

se aplica quando o beneficiário dessa imunidade é posto em causa num processo penal por atos que não foram praticados no âmbito das funções que exerce por conta de uma instituição da União Europeia.

[...]