Privacy and Data Protection Magazine

REVISTA CIENTÍFICA NA ÁREA JURÍDICA

N.º 05 – AGOSTO 2022
REVISTA ONLINE, QUADRIMESTRAL

Direção Executiva
Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez

Universidade Europeia

PRIVACY AND DATA PROTECTION CENTRE

Privacy and Data Protection Magazine

Data: agosto 2022
Publicações: 3 números anuais

ESTATUTO EDITORIAL

1.º Objeto. A Revista Privacy and Data Protection Magazine é uma publicação científica que tem por objeto a Proteção de Dados Pessoais; Direitos Fundamentais; Direito de Propriedade Intelectual, Direito do Consumo, Direito da Saúde, Direito Digital e Inteligência Artificial.

2.º Princípios Deontológicos. Tudo o que, nesta Revista, se venha a publicar, obedecerá rigorosamente à metodologia científica do Direito e à sua praxis quotidiana, sem quaisquer ingredientes políticos ou religiosos. Assim, será sempre no respeito dos princípios deontológicos da imprensa periódica e da ética profissional que se pautará a orientação desta Revista.

3.º Propriedade. É proprietária da Revista a ENSILIS – Educação e Formação, Unipessoal Lda, detentora da Universidade Europeia, com sede na Quinta do Bom Nome, Estrada da Correia, n.º 53, 1500-210.

4.º Edição. A edição da Revista está a cargo da Universidade Europeia.

5.º Objetivo. A Revista visa contribuir para a criação e transmissão do conhecimento científico na área da Proteção de Dados Pessoais; Direitos Fundamentais; Direito de Propriedade Intelectual, Direito do Consumo, Direito da Saúde, Direito Digital e Inteligência Artificial.

6.º Direção Executiva e Editorial. A Revista é dirigida por uma diretora: Cristina Maria de Gouveia Caldeira, que é co-coordenadora do Privacy and Data Protection Centre, email: centro.dataprotection@universidadeeuropeia.pt

7.º Colaborações. A Revista publica em acesso aberto artigos doutrinários e outros estudos, legislação e jurisprudência comentadas e recensões de obras científicas.

8.º Conselho Editorial. Após revisão por pares, a seleção dos trabalhos a publicar é feita por um Conselho Editorial integrados por 6 especialistas de reconhecido mérito.

9.º Periodicidade. A Revista terá periodicidade quadrimestral.

10.º Secções. A Revista compreende quatro secções: (i) Artigos Doutrinários; (ii) Outros Estudos; (iii) Legislação e Jurisprudência Comentadas; (iv) Recensões.

11.º Sistema de Publicação. A Revista com publicação online em três línguas (português, inglês e espanhol), pretende ter um alcance nacional e internacional.

Ficha Técnica

Título
Privacy and Data Protection Magazine

Subtítulo
Revista Científica na Área Jurídica

Número
005

Ano de Publicação
2022

Afiliação
Privacy and Data Protection Centre Universidade Europeia

Autores
Amanda de Castro Cavallaro
Duarte Rodrigues Guerra
Eliseu Filipe Pinto Lopes
Gustavo Rabay Guerra
Leonardo Parentoni
Lurdes Dias Lopes
Pedro Rebelo Botelho Alfaro Velez

Prefácio
Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez

Direção Executiva
Cristina Maria de Gouveia Caldeira

ISSN
2184-920X

Número de Registo
127600

Propriedade
Miguel Carmelo, Gerente único;
ENSILIS - Educação e Formação, Unipessoal, Lda., detida a 100% por Omnymission, Unip. Lda.

Chief Executive Officer
Miguel Carmelo

NIPC/NIF
504 669 788

Editor e Redação
Universidade Europeia, Quinta do Bom Nome, Estrada da Correia, 53, 1500-210, Lisboa

Índice

Prefácio

A revista *Privacy and Data Protection Magazine* prossegue o seu compromisso de publicação regular, em defesa da proteção das pessoas singulares no que se refere ao tratamento dos seus dados pessoais, um direito fundamental, que se afirma, quer por referência aos instrumentos de monitorização e controlo desenvolvidos pelas Autoridade Nacionais de Proteção de Dados, quer pelos mecanismos de gestão e avaliação do risco, que deverão ser adotados por entidades públicas e privadas, sempre que desenvolvam operações de tratamento que representem um risco para o titular dos dados pessoais.

O artigo de abertura sublinha as disposições penais materiais da Lei n.º 79/2021, de 24 de novembro, que transpôs para a ordem jurídica portuguesa a Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, tendo introduzido alterações em vários diplomas legais, entre os quais, a Lei n.º 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime. Ao longo do artigo, o autor critica as modificações introduzidas pela Lei n.º 79/2021 nas disposições penais materiais da Lei 109/2009, bem como os aspetos que o legislador deveria ter corrigido e não corrigiu.

A transformação digital alterou profundamento a vida em sociedade. A omnipresença das tecnologias de informação no quotidiano dos cidadãos, veio permitir a utilização de *Apps*, *Smartphone*, *Cloud*, *Internet of Things*, *Inteligência Artificial*, ao mesmo tempo que a "pegada digital", deixada por nós, por vezes de forma inconciente, vai sendo tratada, com o propósito de estabelecer padrões de comportamento, que alimentam a exploração comercial e originam riscos, ameaças e ataques cibernéticos.

A União Europeia desenhou a sua estratégia digital centrada na aplicação da inteligência artificial em sistemas com um determinado nível de autonomia, de modo a atingir objetivos específicos, justificando na atual publicação, uma crítica ao procedimento legislativo em curso (Regulamento da Inteligência Artificial). Para tal, recorre-se ao método histórico-jurídico, mas com abertura para os métodos comparativo e hermenêutico, demonstra-se como é viável passar de uma perspetiva assente em princípios, para uma perspetiva assente em regras, inclusivamente em um campo tão novo e desafiante como a Inteligência Artificial.

Em sede de "outros estudos" inclui-se um tema de interesse e atualidade permanente, relativo à avaliação de impacto sobre proteção de dados, que encontra acolhimento no artigo 35.º do Regulamento Geral de Proteção de Dados. O autor apresente uma visão técnica e funcional da matéria, que tem evidente interesse aplicativo em organizações públicas e privadas.

Em matéria de Jurisprudência, a publicação contempla um Comentário ao Acórdão do Tribunal da Relação do Porto relativo ao Processo 8233/21.0T8VNG.P1, de 8 de junho de 2022, que na parte que releva para a proteção de dados, entendeu que «A instalação de sistema de geolocalização em táxi, sem visar o controlo do desempenho do motorista (trabalhador), e sem pôr em causa a esfera de privacidade e reserva do motorista (trabalhador), pode ser admitido como meio de prova no procedimento disciplinar.»

Por último, em matéria de recenção são dadas a conhecer duas referências bibliográficas que reativam a filosofica política e jurídica de derivação clássica: Ayuso, Miguel, *¿El pueblo contra el Estado? Las tensiones entre las formas de gobierno y el Estado*, Marcial Pons, Madrid, 2022.

Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez

I_Artigos Doutrinários

Reflexões sobre as alterações às disposições penais materiais da Lei do Cibercrime

Duarte Rodrigues Nunes[1]

RESUMO

A Lei n.º 79/2021, de 24 de novembro, transpôs para a ordem jurídica portuguesa a Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, tendo introduzido alterações em vários diplomas legais, entre os quais, a Lei n.º 109/2009, de 15 de setembro. Nas disposições penais materiais da Lei 109/2009, foram modificados os artigos 3.º e 6.º (que criminalizam a falsidade informática e o acesso ilegítimo) e introduzidos novos tipos de crime nos artigos 3.º-A a 3.º-F, embora algumas das condutas incriminadas nesses novos tipos de crime já fossem punidas como crime na nossa ordem jurídica. E, por força do seu artigo 3.º-G, a Lei n.º 109/2009 abrange os sistemas e meios de pagamento que tenham por objeto moeda virtual (o que inclui as criptomoedas). O presente artigo analisa criticamente as modificações introduzidas pela Lei n.º 79/2021 nas disposições penais materiais da Lei 109/2009 (incluindo se a diretiva foi devidamente transposta), bem como os aspetos que o legislador deveria ter corrigido e não corrigiu.

PALAVRAS-CHAVE:

cibercrime - fraude e contrafação de meios de pagamento diversos do numerário - contrafação de cartões ou outros dispositivos de pagamento – uso de cartões ou outros dispositivos de pagamento contrafeitos - aquisição de cartões ou outros dispositivos de pagamento contrafeitos – aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático.

---

[1] Professor associado convidado da Universidade Europeia. Professor auxiliar convidado da Universidade Lusíada de Angola. Doutor em Direito pela Faculdade de Direito da Universidade de Lisboa. Jurisconsulto. Investigador integrado do Centro de Investigação de Direito Penal e Ciências Criminais e não integrado do Centro de Investigação Jurídica do Ciberespaço, ambos da Faculdade de Direito da Universidade de Lisboa. Autor de 6 monografias (Direito penal e processual penal): Os meios de obtenção de prova da Lei do Cibercrime (2018, Reimpressão: 2020, 2.ª Edição: 2021); Revistas e Buscas no Código de Processo Penal (2019); O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, Tese de Doutoramento (2019); Os crimes previstos na Lei do Cibercrime (2020, Reimpressão: 2021, 2.ª Edição em publicação); Curso de Direito Penal, Parte Geral, Tomo I (2021, 2.ª Edição em publicação); Curso de Direito Processual Penal, Tomo I (em publicação). Autor de mais de 20 artigos em revistas jurídicas (em Portugal e no Estrangeiro) e contributos em obras coletivas em matéria de Direito penal e processual penal (em geral e também – e sobretudo – em matéria de criminalidade organizada, terrorismo, criminalidade económico-financeira, cibercrime, investigação criminal e recuperação de ativos) e Direito civil (Direito das obrigações). Endereço eletrónico: duarterodriguesnunes@hotmail.com

Reflections on the amendments to the substantive criminal provisions of the Cybercrime Law

Duarte Rodrigues Nunes

ABSTRACT

Law no. 79/2021, of 24 November, transposed Directive (EU) 2019/713 of the European Parliament and of the Council, of 17 April 2019, on combating fraud and counterfeiting of non-cash means of payment into Portuguese law, having modified several legislative instruments, including Law no. 109/2009, of 15 September. In the substantive criminal provisions of Law no. 109/2009, articles 3 and 6 (which criminalize computer-related forgery and illegal access) were modified and new statutory offenses were introduced in articles 3-A to 3-F, although some of the conducts provided for and punished by articles 3-A to 3-F were already punished as a crime. According to its article 3-G, Law no. 109/2009 covers payment systems and means of payment whose object is virtual currency (which includes cryptocurrencies). This article analyzes critically the modifications introduced by Law 79/2021 in the substantive criminal provisions of Law no. 109/2009 (including if the Directive was properly transposed), as well as the aspects that the legislator should have corrected and did not correct.

KEYWORDS

cybercrime – fraud and counterfeiting of non-cash means of payment – counterfeiting of payment cards or other payment devices – use of counterfeited payment cards or other payment devices – acquisition of counterfeited payment cards or other payment devices – acquisition of payment cards or other payment devices obtained through computer crimes.

1. Introdução

A Lei n.º 79/2021, de 24 de novembro, que transpôs para a ordem jurídica portuguesa a Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário[2], introduziu diversas alterações no Capítulo II da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), que contém as disposições de Direito penal material dessa Lei As alterações consistiram na alteração de alguns aspetos dos crimes de falsidade informática e de acesso ilegítimo e na introdução de novas incriminações[3].

Todavia, o legislador continua a não observar cabalmente as imposições constantes da **Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto,** relativa a ataques contra os sistemas de informação[4] e que substitui a Decisão-Quadro 2005/222/JAI do Conselho, **apesar de o prazo de transposição da Diretiva já ter decorrido em 04/09/2015[5]. Dado que alguns dos aspetos desse incumprimento têm a ver com o crime de acesso ilegítimo, voltaremos a esta questão quando analisarmos as alterações introduzidas pela Lei n.º 79/2021 no art. 6.º da Lei n.º 109/2009.**

Como se refere na exposição de motivos da Diretiva 2019/713/UE, a fraude e a contrafação de meios de pagamento diversos do numerário constituem uma ameaça à segurança (dado que representam uma fonte de rendimento para a criminalidade organizada e constituem uma forma de facilitar outras atividades criminosas como o terrorismo, o tráfico de estupefacientes e o tráfico de seres humanos) e, concomitantemente, são um obstáculo ao mercado único digital ao minarem a confiança dos consumidores e provocarem prejuízos graves para as vítimas destas atividades criminosas, tornando os cidadãos mais relutantes em efetuar compras online[6]. Fruto do extraordinário desenvolvimento da informática nas últimas décadas, a maior parte desses meios de pagamento diversos do numerário (se não mesmo todos) são meios de pagamento de natureza digital[7], o que os transforma num alvo

---

[2] Doravante, Diretiva 2019/713/UE.

[3] Crimes de contrafação de cartões ou outros dispositivos de pagamento (art. 3.º-A), uso de cartões ou outros dispositivos de pagamento contrafeitos (art. 3.º-B), aquisição de cartões ou outros dispositivos de pagamento contrafeitos (art. 3.º-C), atos preparatórios da contrafação (art. 3.º-D) e aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático (art. 3.º-E), bem como uma agravação do limite mínimo da pena nos casos em que esses crimes sejam cometidos por funcionário no exercício das suas funções (art. 3.º-F), sendo que os sistemas ou meios de pagamento que tenham por objeto moeda virtual (criptomoedas) também se consideram sistema ou meio de pagamento para efeitos da Lei n.º 109/2009 (art. 3.º-G), o que constitui uma importante inovação na nossa legislação.

[4] Doravante, Diretiva **2013/40/UE**.

[5] Cfr., a este respeito, com maiores desenvolvimentos, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 28 e ss.

[6] Cfr. considerandos 1, 2, 7 e 31 da Diretiva 2019/713/UE. Como se refere no mencionado considerando 31 da Diretiva, «*a fraude e a contrafação de meios de pagamento que não em numerário podem ter consequências graves, económicas e não económicas, para as vítimas. Quando a fraude envolve, por exemplo, a usurpação de identidade, as suas consequências são frequentemente agravadas devido por danos ao bom nome, danos profissionais, danos ao bom crédito e danos não patrimoniais graves que acarreta*».

[7] É certo que a Diretiva 2019/713/UE define, no seu art. 2.º, al. a), o "instrumento de pagamento que não em numerário" como «*um dispositivo, objeto ou registo protegido não corpóreo ou corpóreo, ou uma combinação destes elementos, diferente da moeda em curso legal, e que, por si só ou em conjugação com um procedimento ou um conjunto de procedimentos, permite ao titular ou utilizador transferir dinheiro ou valor monetário, inclusive através de meios de troca digitais*» e, nos seus arts. 4.º e 5.º e considerando 15, faz referência às "infrações relacionadas com a utilização fraudulenta de instrumentos de pagamento que não em numerário" tanto corpóreos como não corpóreos (incluindo-se aqui, indubitavelmente, os meios de pagamento *online*, os programas informáticos ou aplicações móveis de pagamento, as *wallets* de criptomoedas, etc.). No entanto, não é porque o meio de pagamento é corpóreo que a informática deixa

preferencial dos cibercriminosos, mormente daqueles cuja atividade criminosa vise a obtenção de lucro, e faz com que a sua atividade criminosa tenha uma relevante dimensão transfronteiriça e decorra em grande parte (ou mesmo exclusivamente) no ciberespaço. E, tendo uma dimensão transfronteiriça, a atividade criminosa relacionada com a fraude e a contrafação de meios de pagamento diversos do numerário irá "contactar" com a ordem jurídica de mais do que um Estado (podendo o criminoso estar num país, a vítima ou as vítimas noutro ou noutros países diferentes e as vantagens do crime serem transferidas, para branqueamento, para um outro país diverso daquele ou daqueles em que se encontram o criminoso e as vítimas), o que, desde logo, dificulta a investigação criminal e, consequentemente, a resposta das autoridades (e a eficácia dessa mesma resposta) a este fenómeno criminoso.

Na medida em que, como referimos, a esmagadora maioria dos meios de pagamento diversos do numerário (se não mesmo todos) são meios de pagamento de natureza digital, podemos afirmar com segurança as atividades criminosas relacionadas com a fraude e a contrafação de meios de pagamento diversos do numerário são levadas a cabo com a utilização de meios informáticos e incidem sobre sistemas informáticos[8] e dados informáticos[9], ou seja, estamos perante cibercrime[10], que, como enfatiza a ONU, é uma forma de crime transnacional em evolução, sendo também uma realidade complexa, decorrendo a sua complexidade do facto de ocorrer no território sem fronteiras do ciberespaço (podendo os agentes e as vítimas estar em países diversos e os efeitos da prática dos crimes produzir-se em todo o Mundo) e do crescente envolvimento de organizações criminosas, gerando a necessidade de criar uma resposta urgente, dinâmica e internacional[11].

E, de facto, pelos lucros que tais atividades podem proporcionar e pelos baixos riscos penais (por força da extrema dificuldade da investigação destas atividades criminosas, maxime se forem levadas a cabo de forma transnacional ou por organizações criminosas, organizações terroristas ou criminosos de colarinho branco[12]), não é difícil antecipar que tal forma de cibercrime (ad latus de outras, igualmente dirigidas à obtenção de lucro, como o phishing, o pharming, o ransomware ou o cryptojacking) seja levada a cabo, não só por criminosos "comuns", mas também por organizações criminosas, criminosos de colarinho branco e organizações terroristas, seja para prosseguir a finalidade lucrativa dos agentes do crime (como na criminalidade económico-financeira) ou para obter financiamento para a prossecução da finalidade

---

de estar em causa, visto que, por exemplo, os dados armazenados na banda magnética ou no *chip* dos cartões de débito ou de crédito são dados informáticos na aceção do art. 2.º, al. b), da Lei n.º 109/2009 ou do art. 2.º, al. b), da Diretiva **2013/40/UE, para o qual o art. 2.º, al. f), da** Diretiva 2019/713/UE remete.

[8] Na aceção do art. 2.º, al. a), da Lei n.º 109/2009.

[9] Na aceção do art. 2.º, al. b), da Lei n.º 109/2009.

[10] Que podemos definir como «o facto tipificado na Lei como crime que é praticado através da utilização de um sistema informático – na aceção do art. 2.º, al. a), da Lei n.º 109/2009 – ou em que o sistema informático é o objeto da ação, ainda que como alvo simbólico, ou dito de outro modo, o facto tipificado na Lei como crime em que o sistema informático é objeto ou instrumento do crime ou cujo cometimento está significativamente ligado à utilização de um sistema informático (cfr. DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 45).

[11] Cfr. DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 14.

[12] Nestes casos, haverá que somar as dificuldades próprias que caracterizam a investigação da criminalidade organizada, do terrorismo e da criminalidade económico-financeira às dificuldades da investigação do cibercrime *ex se*.

última dos agentes do crime (como no terrorismo)[13]. Na verdade, a criminalidade organizada, o terrorismo, a criminalidade económico-financeira e o cibercrime não são realidades estanques entre si, antes possuindo inúmeros vasos comunicantes e áreas de sobreposição e cooperação entre si[14].

Mas, por força do carácter tendencialmente transnacional da atividade criminosa dos cibercriminosos, a resposta ao cibercrime em geral e à fraude e à contrafação de meios de pagamento diversos do numerário em especial também pode ser dificultada (maxime no que diz respeito à cooperação internacional, mas não só) pela existência de diferenças entre a legislação penal dos vários países em causa, bem como de lacunas nessa mesma legislação no que tange à criminalização das condutas, o que realça a necessidade da aproximação da legislação penal nos domínios da fraude e da contrafação de meios de pagamento diversos do numerário, sendo esse o propósito da Diretiva 2019/713/UE[15].

A Diretiva 2019/713/UE abrange as transações com moeda virtual[16], as carteiras digitais (que permitem o armazenamento e a transferência de moedas virtuais), etc., mas não a moeda virtual ex se, devendo os Estados-Membros garantir que o seu Direito interno conferirá às moedas virtuais que venham a ser emitidas por bancos centrais ou por outras autoridades públicas um nível de proteção contra a fraude igual ao nível de proteção de que gozam os meios de pagamento que não em numerário em geral[17].

Com a finalidade de incrementar a eficácia da resposta penal à fraude e à contrafação de meios de pagamento diversos do numerário, a Diretiva inclui também a obrigação de criminalização de condutas que correspondem a atos preparatórios de atos de fraude ou contrafação[18] sem que seja necessária a efetiva utilização

---

[13] No caso da criminalidade organizada, a sua finalidade tanto pode ser a obtenção de lucro (como sucederá na maioria das situações) como outra finalidade (lícita ou ilícita), não se justificando limitar a finalidade da criminalidade organizada à obtenção de lucro, ainda que essa seja a finalidade que é prosseguida na maioria das situações (cfr., a este respeito, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 122 e ss.).

[14] Acerca do modo como a criminalidade organizada, o terrorismo e a criminalidade económico-financeira fazem uso do cibercrime na preparação e/ou execução dos crimes e/ou no apagamento dos vestígios do cometimento dos crimes, *vide* DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 29 e ss.

[15] Cfr. art. 1.º e considerandos 5, 6 e 8 da Diretiva 2019/713/UE. Como resulta do art. 1.º e do considerando 18, a Diretiva prevê regras mínimas, permitindo que os Estados-Membros adotem ou mantenham regras de Direito penal mais rigorosas quanto à fraude e contrafação de meios de pagamento diversos do numerário, incluindo no que tange a uma definição mais ampla das infrações.

[16] Definida, no art. 2.º, al. d), da Diretiva 2019/713/UE, como «uma representação digital de valor que não é emitida nem garantida por um banco central ou uma autoridade pública, não está necessariamente ligada a uma moeda legalmente estabelecida e não possui o estatuto jurídico de moeda ou dinheiro, mas que é aceite por pessoas singulares ou coletivas como meio de troca e pode ser transferida, armazenada e comercializada por via eletrónica».

[17] Cfr. considerando 10.

[18] Como sejam a recolha e a posse de instrumentos de pagamento com intenção de cometer uma fraude através, por exemplo, de *phishing*, *skimming* ou do redirecionamento dos utilizadores de serviços de pagamento para páginas *Web* falsas, a posse, aquisição e distribuição de *malware* ou de dados relativos a cartões de crédito ou débito ou de serviços de *homebanking* (*maxime* códigos pessoais e *passwords*), etc., mas sem que a Diretiva imponha, no caso da posse de dispositivos, a criminalização da simples omissão (cfr. considerando 13). À semelhança do que sucedeu na Convenção sobre o Cibercrime do Conselho da Europa (cfr. art. 6.º), a Diretiva apenas impõe a criminalização no caso de dispositivos que sejam principalmente concebidos ou especificamente adaptados para cometer as infrações referidas na Diretiva, não a impondo no caso de dispositivos de utilização dupla (*i.e.*, os dispositivos que, não sendo exclusiva ou especificamente concebidos para a prática de infrações, poderão ser utilizados para essa finalidade) (cfr. art. 7.º e considerando 16); todavia, uma vez que a Diretiva apenas prevê regras mínimas, nada impede que os Estados-membros, no seu Direito interno, criminalizem a posse, aquisição e distribuição de dispositivos

fraudulenta dos meios de pagamento diversos do numerário[19]. A Diretiva apenas impõe a criminalização no caso de condutas dolosas[20], mas, por outro lado, prevê uma obrigação de criminalizar a instigação, a cumplicidade e a tentativa nos termos referidos no seu art. 8.º.

De acordo com o considerando 19 da Diretiva, o legislador europeu considera adequada a agravação das sanções quando um dos crimes nela previstos seja cometido no contexto de uma organização criminosa, na aceção da Decisão-Quadro 2008/841/JAI do Conselho, de 24 de outubro de 2008, relativa à luta contra a criminalidade organizada[21] (prevendo uma pena cujo limite máximo deverá de ser de, pelo menos, 5 anos[22]), a menos que o Direito interno já preveja sanções mais severas do que as previstas na Diretiva. Ainda de acordo com o mesmo considerando, quando uma infração prevista na Diretiva tenha sido cometida em conjugação com outra infração também prevista na mesma e praticada pelo mesmo agente e a conduta que configure a prática de uma dessas infrações constitua um elemento típico da outra, os Estados-Membros poderão, de acordo com os princípios gerais do Direito interno, determinar que essa conduta seja considerada como circunstância agravante da infração principal.

A Diretiva impõe a criminalização da utilização fraudulenta de instrumentos de pagamento diversos do numerário quando praticada com dolo (art. 3.º), a utilização fraudulenta de instrumentos de pagamento corpóreos e não corpóreos diversos do numerário quando praticada com dolo (arts. 4.º e 5.º), a fraude relacionada com sistemas de informação quando praticada com dolo (art. 6.º), a produção, aquisição, importação, exportação, venda, transporte, distribuição ou disponibilização de um dispositivo ou instrumento, dados informáticos ou outros meios principalmente concebidos ou especificamente adaptados para cometer uma das infrações previstas nos arts. 4.º, als. a) e b), 5.º, als. a) e b), e 6.º, pelo menos quando esses atos forem praticados com a intenção de que esses meios sejam utilizados (art. 7.º), sob qualquer forma de autoria ou participação e na forma consumada ou tentada (cfr. art. 8.º) e independentemente de o agente do crime ser uma pessoa singular ou uma pessoa coletiva[23], desde que, neste último caso, (1) a infração tenha sido cometida em

---

de utilização dupla desde que se prove que essa posse, aquisição ou distribuição se destinava à ulterior prática de crimes.

[19] Cfr. art. 7.º e considerando 13.

[20] Cfr. considerando 14. Todavia, ao apenas prever regras mínimas, a Diretiva não impede que os Estados-membros, no seu Direito interno, criminalizem algumas dessas condutas também a título de negligência, o que, de todo o modo, não sucede no Direito português, em que as condutas são punidas apenas a título de dolo.

[21] De acordo com o art. 1.º desta Decisão-Quadro, a organização criminosa consiste numa «associação estruturada de mais de duas pessoas, que se mantém ao longo do tempo e atua de forma concertada, tendo em vista a prática de infrações passíveis de pena privativa de liberdade ou medida de segurança privativa de liberdade cuja duração máxima seja, pelo menos, igual ou superior a quatro anos, ou de pena mais grave, com o objetivo de obter, direta ou indiretamente, benefícios financeiros ou outro benefício material», ao passo que a associação estruturada consiste n' «uma associação que não foi constituída de forma fortuita para a prática imediata de uma infração e que não tem necessariamente atribuições formalmente definidas para os seus membros, continuidade na sua composição ou uma estrutura sofisticada».

[22] Cfr. art. 9.º, n.º 6.

[23] Definida, no art. 2.º, al. g), da Diretiva, como «uma entidade dotada de personalidade jurídica ao abrigo do direito aplicável, com exceção dos Estados ou de organismos públicos no exercício de prerrogativas de autoridade pública e das organizações internacionais públicas».

benefício da pessoa coletiva por qualquer pessoa, agindo a título individual ou como membro de um órgão da pessoa coletiva e que nela ocupe uma posição de liderança, com base no poder de representação da pessoa coletiva ou em poderes de autoridade para tomar decisões em nome da pessoa coletiva ou para exercer controlo sobre essa pessoa coletiva ou (2) a prática da infração em benefício da pessoa coletiva, por uma pessoa sob a sua autoridade, tenha sido possível em virtude da falta de supervisão ou de controlo por parte de uma dessas pessoas (cfr. art. 10.º, n.ºs 1 e 2). Além disso, a Diretiva prevê as penas aplicáveis às pessoas singulares e coletivas (cfr. arts. 9.º e 11.º), sendo que, no caso das pessoas singulares fixa o quantum mínimo dos limites máximos das penas que deverão ser aplicadas às infrações previstas nos arts. 3.º e ss. (cfr. art. 9.º, n.ºs 2 a 6).

O legislador, na Lei 79/2021, optou (a nosso ver, corretamente) por reorganizar as normas penais que circunscrevem a criminalidade respeitante a meios de pagamento, constando do Código Penal (como já constavam) as normas que se referem a meios de pagamento em numerário (papel-moeda ou moeda metálica) e ao uso abusivo de meios de pagamento eletrónicos autênticos e da Lei do cibercrime todas as normas penais respeitantes a manipulações informáticas abusivas de meios de pagamento eletrónicos não corpóreos[24].

2. As alterações introduzidas no artigo 3.º da Lei n.º 109/2009 (crime de falsidade informática)

No caso do crime de falsidade informática, as alterações do art. 3.º da Lei n.º 109/2009[25] consistiram em:

a) retirar do n.º 2 a conduta de "introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, sempre que os dados que sejam alvo dessa manipulação estejam registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento", que passou a ser p. e p. pelo art. 3.º-A dessa mesma Lei e, além disso, as condutas de "produzir, adquirir, importar, distribuir, vender ou deter qualquer dispositivo, programa ou outros dados informáticos destinados a introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, sempre que os dados que sejam alvo dessa manipulação estejam registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento" passaram punidas a ser à luz do art. 3.º-D da mesma Lei;

b) retirar da 2.ª parte do n.º 3 a conduta de "usar documento produzido a partir de dados informáticos registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou

[24] No mesmo sentido, PROCURADORIA-GERAL DA REPÚBLICA, Nota Prática n.º 24/2021, pp. 5-6.

[25] Acerca das cinco condutas típicas do crime de falsidade informática, p. e p. pelo art. 3.º da Lei n.º 109/2009, *vide* DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 51 e ss.

meio de pagamento e que foram objeto de introdução, modificação, apagamento ou supressão ou cujo tratamento informático foi alvo de interferência por qualquer outra forma", que passou a ser punida à luz do art. 3.º-B dessa mesma Lei;

c) reformular o n.º 4, passando a incluir os atos de produzir e adquirir e não limitar a detenção aos casos em que se destine a fins comerciais (passando a abranger a detenção para qualquer fim, designadamente para uso pessoal do próprio detentor)[26].

Deste modo, o art. 3.º, n.º 2, da Lei n.º 109/2009 passou a incluir apenas a conduta de "introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, sempre que os dados que sejam alvo dessa manipulação estejam registados ou incorporados em dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado"[27], ao passo que a 2.ª parte do n.º 3 desse mesmo preceito passou a incluir apenas a conduta de "usar documento produzido a partir de dados informáticos registados ou incorporados em dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado e que foram objeto de introdução, modificação, apagamento ou supressão ou cujo tratamento informático foi alvo de interferência por qualquer outra forma".

No entanto, além do que referimos supra quanto às alterações do art. 3.º, n.º 4, o legislador não aproveitou a oportunidade para suprir outros aspetos menos positivos de que, na nossa opinião, esse mesmo art. 3.º, n.º 4, padecia e continua a padecer[28].

3. As alterações introduzidas no artigo 6.º da Lei n.º 109/2009 (crime de acesso ilegítimo)

Por seu turno, as alterações introduzidas pela Lei n.º 79/2021 no artigo 6.º da Lei n.º 109/2009 são mais significativas do que no caso das alterações ao art. 3.º da mesma Lei, que acabámos da analisar.

Deste modo, a Lei n.º 79/2021 alterou o art. 6.º da Lei n.º 109/2009 nos seguintes termos:

---

[26] Tendo acolhido as nossas críticas/sugestões a esse respeito (cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 68 e ss.

[27] No caso de dados informáticos registados ou incorporados em dispositivo que permita o acesso a sistema de comunicações, trata-se de dados informáticos que permitem aceder a uma rede de dispositivos na qual circulam informações entre um emissor e um recetor, independentemente de se tratar de sistemas de comunicação por cabo ou *Wireless*, cabendo aí uma plêiade de realidades como as comunicações via satélite, telefónicas (fixas ou móveis), sistemas de distribuição de sinal de televisão por cabo, *Wired Networks*, etc. (cfr. PEDRO VERDELHO, "A nova Lei do Cibercrime", *in* SciVr, T. LVIII, p. 725, e DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 59-60).

Por seu turno, no caso dos dados informáticos registados ou incorporados em dispositivo que permita o acesso a serviço de acesso condicionado, trata-se de serviços que, ou não estão acessíveis ao público em geral ou, estando, implicam, por exemplo, o pagamento de uma contrapartida específica (*v.g.*, monetária), podendo estar em causa, por exemplo, a falsificação de cartões SIM, que, combinados com *hardware*, permitam aceder a sistemas de comunicações (cfr. DUARTE RODRIGUES NUNES, *Idem*, p. 60).

[28] Acerca desta questão, que não importa aprofundar neste artigo (atento o objeto do mesmo) *vide* DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 65 e ss.

a) introduziu, no n.º 3 desse preceito, uma nova circunstância modificativa agravante do crime de acesso ilegítimo (passando a pena a ser pena de prisão até 2 anos[29] ou de multa até 240 dias em vez de pena prisão até 1 ano ou de multa até 120 dias aplicável aos casos subsumíveis aos n.ºs 1 e 2 do mesmo preceito), que consiste em produzir, vender, distribuir ou, por qualquer outra forma, disseminar ou introduzir, num ou mais sistemas informáticos, dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a permitir o acesso, de qualquer modo, a um sistema informático, com a finalidade de obter dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento;

b) criou uma nova circunstância modificativa agravante do crime de acesso ilegítimo no atual n.º 4 (antigo n.º 3) desse preceito (sendo punível com pena de prisão até 3 anos[30]), que consiste em o agente ter obtido, através do acesso não autorizado, dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento;

c) afastou a punibilidade da tentativa também nos casos subsumíveis ao novo n.º 3 desse preceito (anteriormente, essa exclusão já incluía as situações subsumíveis ao n.º 2) (cfr. art. 6.º, n.º 6); e

d) tendo em conta as alterações introduzidas na numeração do art. 6.º, modificou o novo n.º 7 (anterior n.º 6) desse preceito, passando a previsão da necessidade de apresentação de queixa para a instauração do procedimento criminal a abranger as situações subsumíveis aos n.ºs 1, 4 (anterior n.º 3, com a inclusão da nova conduta referida em b)) e 6 (anterior n.º 5).

No que diz respeito às novas condutas típicas constantes do art. 6.º, n.ºs 3 e 4, al. b), da Lei n.º 109/2009, trata-se da criminalização de atos preparatórios de condutas que, do ponto de vista estrutural, constituem atos preparatórios de condutas de fraude e/ou contrafação de meios de pagamento, cuja obrigação de criminalização resulta do art. 7.º da Diretiva 2019/713/UE (expressamente, no caso do n.º 3, e, por interpretação extensiva, por maioria de razão, no caso da al. b) do n.º 4). Todavia, tanto no caso dos n.ºs 2 (para cujas condutas aí elencadas o n.º 3 remete) e 3, o legislador português continua a não suprir a omissão de transposição cabal dos arts. 6.º da Convenção sobre o Cibercrime do Conselho da Europa [31,32] e 7.º da Diretiva 2013/40/UE[33] e não transpõe

[29] Esta pena abstrata observa a imposição do art. 9.º, n.º 5, da Diretiva 2019/713/UE.

[30] Tal pena abstrata também respeita a imposição do art. 9.º, n.º 2, da Diretiva 2019/713/UE, sem prejuízo do que referiremos infra quanto aos casos em que a infração seja cometida no contexto de uma organização criminosa.

[31] Doravante, CCiber.

[32] Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 28 e 164.

[33] Aliás, o legislador continua a não suprir uma outra falta de transposição da Diretiva 2013/40/UE relativamente ao crime de acesso ilegítimo, mais concretamente, o legislador ainda não transpôs devidamente o disposto no art. 9.º, n.ºs 1 e 2, dessa Diretiva (na parte em que se refere às condutas de acesso ilícito a sistemas de informação, previsto no seu art. 3.º e em que impõe a punição com uma pena de, pelo menos, 2 anos de prisão nos casos que se revistam de alguma gravidade). Na verdade, a conduta prevista no art. 6.º, n.º 1, da Lei n.º 109/2009 (ao qual são subsumíveis os casos em que o prejuízo causado é

cabalmente o art. 7.º da Diretiva 2019/713/UE (neste último caso, porque o art. 6.º, n.º 2, para o qual o n.º 3 remete, não inclui as condutas de aquisição, para o agente ou um terceiro, e de importação de dispositivos, o que deverá ser corrigido o mais brevemente possível).

Como referimos, as novas condutas típicas constantes do art. 6.º, n.ºs 3 e 4, al. b), da Lei n.º 109/2009 consistem na criminalização de condutas que, do ponto de vista estrutural, constituem atos preparatórios de condutas de fraude e/ou contrafação de meios de pagamento. No fundo, está em causa o acesso (ou a preparação/facilitação/possibilitação desse acesso através da adoção de alguma das condutas previstas no n.º 2 desse preceito) e a obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento [v.g., dados informáticos incorporados num cartão de débito ou crédito, numa wallet de criptomoedas, em dispositivos de hardware (computadores, tablets, smartphones, suportes autónomos, como uma pendrive, etc.) que permitam o acesso a redes de pagamentos ou transferências de dinheiro como as redes Multibanco, Visa, Mastercard, American Express ou Paypal, plataformas de trading de criptomoedas, etc.].

No que concerne especificamente ao art. 6.º, n.º 3, não percebemos o porquê de a agravação aí prevista só abranger as condutas de produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a proporcionar o acesso sem permissão legal ou sem a autorização do proprietário ou de outro titular do direito do sistema ou de parte dele (acesso ilegítimo) a um sistema informático e não também a conduta de aceder ilegitimamente a um sistema informático com a finalidade de obter dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento[34].

Mas, mais do que isso, a agravação decorrente da atuação com a finalidade de obter dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento também quanto à conduta de aceder ilegitimamente a um sistema informático (p. e p. pelo art. 6.º, n.º 1) também constitui um ato estruturalmente preparatório de condutas de fraude e/ou contrafação de meios de pagamento diversos do numerário[35], inclusivamente mais "próximo" dessas condutas do que os atos

---

de valor elevado) é punível com uma pena até 1 ano de prisão, pelo que as exigências da referida Diretiva apenas serão cabalmente cumpridas se, no n.º 4 do art. 6.º da Lei n.º 109/2009, se incluírem os casos em que o prejuízo causado seja de valor elevado (que, na nossa ótica, são casos que se revestem de alguma gravidade) ou se, no mínimo, se inserisse um novo número no preceito, nos termos do qual, em tais casos, a conduta passasse a ser punível com uma pena de prisão até 2 anos (cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 28-29).

[34] Por seu turno, em PROCURADORIA-GERAL DA REPÚBLICA, Nota Prática n.º 24/2021, pp. 10-11, parece considerar-se (a nosso ver, sem razão, tendo em conta a letra da lei) que, no art. 6.º, n.º 3, da Lei n.º 109/2009, está em causa a punição do acesso ilegítimo e não as condutas de produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a proporcionar o acesso sem permissão legal ou sem a autorização do proprietário ou de outro titular do direito do sistema ou de parte dele (acesso ilegítimo) a um sistema informático.

[35] Na verdade, a conduta do crime de acesso ilegítimo prevista no art. 6.º, n.º 1, da Lei n.º 109/2009, além de constituir crime *ex se* (possuindo o simples acesso não autorizado a um sistema informático dignidade e carência de tutela penal em face da lesão de bens jurídicos que representa), facilita ou pode facilitar o cometimento de outros crimes, podendo a criminalização do acesso ilegítimo ser vista também como uma

mencionados no n.º 2 do art. 6.º (conjugado com o n.º 3 desse mesmo preceito) e, por isso, a admissibilidade da antecipação da tutela penal até será menos discutível[36].

No fundo, de jure condendo, a expressão "as ações descritas no número anterior" constante do art. 6.º, n.º 3, deveria ser substituída pela expressão "as ações descritas nos números anteriores", assim se transpondo cabalmente a Diretiva.

As condutas referidas no art. 6.º, n.º 3, da Lei n.º 109/2009, tal como sucede com as do n.º 2, terão de ser levadas a cabo de forma ilegítima, ou seja, o agente terá de atuar sem permissão legal ou sem autorização do proprietário ou de outro titular do direito do sistema ou de parte dele[37].

No que diz respeito aos dispositivos incluídos no art. 6.º, n.º 3, da Lei n.º 109/2009, esta norma, tal como o n.º 2[38], inclui os dispositivos concebidos exclusiva ou especificamente para a prática de infrações e os que, não sendo exclusiva ou especificamente concebidos para a prática de infrações, poderão ser utilizados para essa finalidade, sem prejuízo de, neste último caso, ser necessário provar que se destinam a ser utilizados para aceder ilegitimamente a um sistema informático alheio

---

proteção antecipada e indireta contra os danos que afetem dados informáticos e/ou a espionagem informática (cfr. LOPES ROCHA, "A lei da criminalidade informática (Lei n.º 109/01 de 17 de Agosto). Génese e técnica legislativa", *in* Cadernos de Ciência de Legislação, n.º 8, p. 75, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 152-153, PEDRO VERDELHO/ROGÉRIO BRAVO/MANUEL LOPES ROCHA, Leis do Cibercrime, I, p. 254, PEDRO SIMÕES DIAS, "O "Hacking" enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo Direito", *in* Direito da Sociedade da Informação, VIII, pp. 254 e ss., JOÃO CARLOS CRUZ BARBOSA DE MACEDO, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, p. 245, e Acórdãos da RG de 17/11/2008 e da 1.ª Vara Mista da Comarca de Guimarães de 26/06/2007).

[36] Sem que estejamos a questionar a admissibilidade da antecipação da tutela penal prevista no art. 6.º, n.º 3, da Lei n.º 109/2009, que, a nosso ver, se justifica plenamente.

[37] Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 164-165. No que se refere às condutas referidas no art. 6.º, n.º 2, da lei n.º 109/2009, dispõe o art. 6.º, n.º 2, da CCiber que «*O presente artigo não pode ser interpretado no sentido de determinar que existe responsabilidade criminal nos casos em que a finalidade da produção, venda, obtenção para utilização, importação, distribuição ou outras formas de disponibilização referidas no n.º 1 do presente artigo não é a prática de uma das infrações previstas nos artigos 2.º a 5.º da presente Convenção, mas antes a realização de testes autorizados ou a proteção de um sistema informático*.». E diz-se no Relatório Explicativo da Convenção sobre o Cibercrime: «*O parágrafo 2 define, claramente, que as ferramentas criadas para a execução de operações autorizadas de teste ou de proteção de sistemas informáticos não se encontram cobertas pela presente disposição. Este conceito é já subjacente à expressão "sem direito". Por exemplo, os dispositivos de teste (dispositivos de cracking) e os dispositivos de análise de redes concebidos por este sector da indústria, com o objetivo de controlar a fiabilidade dos seus produtos de tecnologia da informação, ou de testar a segurança dos seus sistemas, são fabricados para fins legítimos, pelo que se considera serem utilizados "com direito"*.».

Por seu turno, no que concerne às condutas previstas no art 6.º, n.º 3, da Lei n.º 109/2009, diz-se, no considerando 13 da Diretiva 2019/713/UE, que «*É especialmente necessária uma abordagem comum no direito penal relativamente aos elementos constitutivos da conduta criminosa que contribuem para a efetiva utilização fraudulenta dos meios de pagamento que não em numerário ou que são preparatórios relativamente a essa utilização. Condutas como a recolha e a posse de instrumentos de pagamento com intenção de cometer uma fraude através, por exemplo, de phishing (mistificação da interface), skimming (clonagem) ou do (re)direcionamento dos utilizadores de serviços de pagamento para falsos sítios Web, e respetiva distribuição (por exemplo, através da venda de informações sobre cartões de crédito na Internet) deverão portanto configurar um tipo de infração penal por direito próprio sem que seja necessária a efetiva utilização fraudulenta dos meios de pagamento que não em numerário (…). A presente diretiva não deverá impor sanções à utilização legítima de um instrumento de pagamento, inclusive e em relação à prestação de serviços de pagamento inovadores, tais como os serviços habitualmente desenvolvidos pelas empresas ligadas às tecnologias financeiras*», daqui resultando que, pelo menos por igualdade de razão, tal Diretiva não impõe a criminalização da produção, venda, distribuição ou disseminação ou introdução, por qualquer meio, num sistema informático, de dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a permitir o acesso a um sistema informático para obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento quando tal ocorra ao abrigo de uma permissão legal ou com a autorização do proprietário ou de outro titular do direito do sistema ou de parte dele.

[38] Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 163.

com a finalidade de obter dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento. Na verdade, ainda que se refira, no art. 7.º e no considerando 16 da Diretiva 2019/713/UE, que a mesma apenas impõe a criminalização no caso de dispositivos que sejam principalmente concebidos ou especificamente adaptados para cometer as infrações referidas nos seus arts. 3.º a 6.º, essa mesma Diretiva impõe apenas regras mínimas (cfr. art. 1.º e considerando 18) e o legislador português não opera qualquer distinção entre "dispositivos concebidos exclusiva ou especificamente para permitir o acesso a sistema ou meio de pagamento" e "dispositivos que, não tendo sido concebidos exclusiva ou especificamente para permitir o acesso a sistema ou meio de pagamento, ainda assim possam ser utilizados também para essa finalidade" (dispositivos de utilização dupla).

E, atenta a ratio antecipatória da tutela penal do art. 6.º, n.ºs 2 e 3, não se perceberia o porquê de uma tal distinção, dado que ambos os tipos de dispositivos acabam por permitir o acesso a sistemas ou meios de pagamento, gerando, desse modo, um especial perigo para o bem jurídico tutelado pela incriminação que justifica uma tal antecipação da tutela penal.

Ademais, se, no art. 276.º do CP, o legislador apenas incrimina a importação, o fabrico, a guarda, a compra, a venda, a cedência ou a aquisição a qualquer título, o transporte, a distribuição e a detenção de "instrumento ou aparelhagem especificamente destinados à montagem de escuta telefónica ou à violação de correspondência ou de telecomunicações", caso pretendesse que o art. 6.º, n.ºs 2 e 3, da Lei n.º 109/2009 apenas se aplicasse aos dispositivos concebidos exclusiva ou especificamente para permitir o acesso a sistema ou meio de pagamento, tê-lo-ia feito, adotando uma formulação análoga à que adotou no art. 276.º do CP, mas não o fez.

Daí que, por aplicação do princípio ubi lex non distinguit nec nos distinguere debemus, consideremos que o art. 6.º, n.º 3, da Lei n.º 109/2009 inclui também os dispositivos de utilização dupla, embora com a exigência adicional a que fizemos referência.

O bem jurídico tutelado pelo crime de acesso ilegítimo é a segurança dos sistemas informáticos, sem prejuízo de, reflexamente, acabar por proteger outros bens jurídicos como a intimidade/privacidade, o património, a concorrência e a liberdade de comércio[39,40], sendo que a introdução das condutas previstas nos n.ºs 3 e 4, al. b), do art. 6.º nada altera a este respeito.

No caso da conduta prevista no art. 6.º, n.º 3, da Lei n.º 109/2009, o crime de acesso legítimo constitui um crime de perigo abstrato (quanto ao grau de lesão do bem jurídico) e de mera atividade (quanto à modalidade de consumação do ataque ao bem jurídico), pois não ocorre qualquer lesão efetiva do bem jurídico (mas apenas a produção, venda, distribuição ou disseminação ou introdução, por qualquer meio, num sistema informático, de dispositivos, programas, um conjunto executável de instruções,

---

[39] Pois, através da intromissão no sistema e do consequente acesso aos dados aí guardados, o agente poderá, *eventualmente*, tomar conhecimento de informações relativas ao segredo comercial ou industrial ou de cariz íntimo ou privado ou obter benefícios económicos e, concomitantemente, gerar prejuízos económicos; contudo, a punição do acesso ilegítimo não assenta nessas circunstâncias *eventuais*, mas no simples acesso ilegítimo a um sistema informático alheio.

[40] Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 157. Acerca dos vários entendimentos na Doutrina e na Jurisprudência quanto ao bem jurídico tutelado pelo crime de acesso ilegítimo, *vide* DUARTE RODRIGUES NUNES, *Idem*, p. 156.

um código ou outros dados informáticos destinados a permitir o acesso a um sistema informático para obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento) nem se verifica qualquer modificação do mundo exterior[41].

No que tange à não punição da conduta prevista no art. 6.º, n.º 3, da Lei n.º 109/2009, vale aqui mutatis mutandis a crítica que formulamos à opção do legislador no que tange à conduta prevista no n.º 2 desse preceito[42]. Mas, existe um argumento adicional: nos termos do art. 8.º, n.º 2, da Diretiva 2019/713/UE, o legislador comunitário impõe a criminalização da tentativa de cometimento, entre outros, da infração prevista no art. 5.º, al. a), dessa mesma Diretiva, sendo que, como referimos, o art. 5.º, al. a), da Diretiva 2019/713/UE, razão pela qual entendemos que o art. 8.º, n.º 2, conjugado com o 5.º, al. a), impõe a criminalização da conduta prevista no art. 6.º, n.º 3, da Lei n.º 109/2009 também na forma tentada.

Passando à conduta criminalizada pelo art. 6.º, n.º 4, al. b), da Lei n.º 109/2009, o agente, além de levar a cabo um acesso ilegítimo a um sistema informático, obtém dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, agravando a lesão do bem jurídico que já resultava do "mero" acesso ilegítimo.

No caso da conduta prevista no art. 6.º, n.º 4, al. b), o crime de acesso legítimo constitui um crime de dano (quanto ao grau de lesão do bem jurídico) e de mera atividade (quanto à modalidade de consumação do ataque ao bem jurídico), pois a lei exige que o agente obtenha efetivamente dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, mas, por outro lado, a conduta do agente não produz qualquer modificação do mundo exterior.

Relativamente à relação entre as condutas p. e p. pelo art. 6.º, n.º 3, e pelo art. 6.º, n.º 4, al. b), em que, para além da intenção de obter dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento (que o n.º 3 exige), há um efetivo acesso ilegítimo e, mais do que isso, o agente logra obter dados dessa natureza (o que incrementa ainda mais a lesão do bem jurídico e justifica uma agravação do limite máximo da pena aplicável ainda maior do que no caso do n.º 3), consideramos que existe uma relação de concurso aparente de crimes, mais concretamente de consunção, em que a conduta p. e p. pelo art. 6.º, n.º 4, al. b), consome a conduta p. e p. pelo art. 6.º, n.º 3 (que apenas funcionará como

[41] Cfr. embora referindo-se ao n.º 2 (para o qual o n.º 3 remete) do art. 6.º da Lei n.º 109/2009, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 158.

[42] Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 172. No fundo, consideramos que, *de jure condendo*, pela enorme perigosidade objetiva que os atos de produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a permitir o acesso a sistemas informáticos encerram e tendo em conta a lógica preventiva que presidiu à construção do tipo de crime de acesso ilegítimo, justificar-se-ia a punição da tentativa nos casos previstos no n.º 2 do art. 6.º da Lei n.º 109/2009.

circunstância a valorar em sede de determinação da medida concreta da pena, nos termos do art. 71.º, n.º 2, do CP)[43].

Por último, nos termos do art. 9.º, n.º 6, da Diretiva 2019/713/UE, «Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infrações previstas nos artigos 3.º a 6.º sejam puníveis com uma pena de prisão máxima não inferior a cinco anos se forem cometidas no contexto de uma organização criminosa, na aceção da Decisão-Quadro 2008/841/JAI, independentemente da sanção prevista nessa decisão».

Apreciando a observância, ou não, desta imposição na Lei n.º 79/2021, no caso do art. 6.º, n.º 3, da Lei n.º 109/2009, está em causa a transposição do art. 7.º da Diretiva, pelo que a imposição prevista no art. 9.º, n.º 6, não se aplica. Mas o mesmo já não sucede no caso do art. 6.º, n.º 4, al. b), pois o limite máximo da pena aplicável é de 3 anos sem se prever uma pena de prisão de, pelo menos, até 5 anos no caso de o crime ser cometido no contexto de uma organização criminosa[44], o que constitui um outro caso de transposição defeituosa da Diretiva.

4. O novo crime de contrafação de cartões ou outros dispositivos de pagamento (artigo 3.º-A da Lei n.º 109/2009).

Nos termos do art. 3.º-A da Lei n.º 109/2009, «Quem, com intenção de provocar engano nas relações jurídicas, contrafizer cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, nomeadamente introduzindo, modificando, apagando, suprimindo ou interferindo, por qualquer outro modo, num tratamento informático de dados registados, incorporados, ou respeitantes a estes cartões ou dispositivos, é punido com pena de prisão de 3 a 12 anos», sendo a pena aplicável de prisão entre 4 e 12 anos no caso de o crime ser cometido por funcionário no exercício das suas funções (cfr. art. 3.º-F, al. b))[45].

A consagração legal do crime de contrafação de cartões ou outros dispositivos de pagamento foi acompanhada pela supressão da referência à manipulação de dados informáticos registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento ou do seu tratamento no art. 3.º, n.º 2, da Lei n.º 109/2009 e também pela modificação do art. 267.º, n.º 1, al. c), do CP, que passou pela supressão da equipação dos cartões de crédito à moeda para efeitos dos crimes de falsificação de moeda falsa, p. e p. pelos arts. 262.º a 266.º do CP.

Até à Lei n.º 79/2021 suscitava-se a questão de saber se o art. 3.º, n.º 2, da Lei n.º 109/2009 revogara, ou não, a norma resultante da conjugação do art. 262.º com o art. 267.º, n.º 1, al. c), ambos do CP, na parte em que se referiam aos cartões de crédito, sendo que, caso se concluísse que tal revogação ocorrera, a contrafação de cartões

---

[43] Relativamente à relação entre as condutas p. e p. pelo art. 6.º da Lei n.º 109/2009, embora na versão anterior à Lei n.º 79/2021, *vide* DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 176-177.

[44] *In casu*, uma associação criminosa, tal como prevista no art. 299.º do CP, e/ou uma organização terrorista, tal como prevista no art. 2.º da Lei n.º 52/2003, de 22 de agosto.

[45] As penas abstratas de 3 a 12 e de 4 a 12 anos observam a imposição do art. 9.º, n.º 2, da Diretiva 2019/713/UE.

de crédito teria passado a ser punida com uma pena entre 1 e 5 anos em lugar de ser punida com uma pena entre 3 e 12 anos de prisão, o que mal se compreenderia[46].

Consideramos que, no que tange ao novo crime de contrafação de cartões ou outros dispositivos de pagamento (p. e p. pelo art. 3.º-A da Lei n.º 109/2009) e à modificação do art. 267.º, n.º 1, al. c), do CP que mencionámos, a solução introduzida pela Lei n.º 79/2021 resolveu a questão de forma correta, daí resultando uma equiparação, do ponto de vista das consequências jurídicas, da contrafação de cartões de crédito à contrafação de moeda.

O art. 3.º-A da Lei n.º 109/2009 (tal como já sucedia com o art. 3.º, n.º 2, da mesma Lei na versão anterior à Lei n.º 79/2021[47]), ao contrário do art. 267.º, n.º 1, al. c) do CP[48], inclui igualmente a contrafação de cartões de débito. Contudo, até à entrada em vigor do novo art. 3.º-A da Lei n.º 109/2009, a contrafação de cartões de débito e de outros meios de pagamento diversos do numerário era punida com pena de prisão entre 1 e 5 anos, ao passo que a contrafação de cartões de crédito era punida com uma pena entre 3 e 12 anos[49]. Deste modo, a lei veio – a nosso ver bem – equiparar a contrafação de cartões de crédito e de débito em termos de pena aplicável[50], que, por sua vez, é exatamente igual à pena aplicável ao crime de contrafação de moeda[51].

Além dos cartões de crédito e de débito, o art. 3.º-A da Lei n.º 109/2009 inclui também os demais sistemas e meios eletrónicos de pagamento (obviamente diversos do numerário), incluindo a moeda virtual (cfr. art. 3.º-G), definida, no art. 2.º, al. d), da Diretiva 2019/713/UE, como «uma representação digital de valor que não é emitida nem garantida por um banco central ou uma autoridade pública, não está necessariamente ligada a uma moeda legalmente estabelecida e não possui o estatuto jurídico de moeda ou dinheiro, mas que é aceite por pessoas singulares ou coletivas como meio de troca e pode ser transferida, armazenada e comercializada por via eletrónica», que

---

[46] Acerca desta questão, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 60 e ss.

[47] Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 59, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, p. 1027, e Acórdãos da RL de 30/06/2011 e 10/07/2012.

[48] Cfr. PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, p. 1027, ALMEIDA COSTA, "Art. 267º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, pp. 811-812, e Acórdãos da RL de 30/06/2011 e 10/07/2012.

[49] A equiparação do cartão de crédito à moeda para efeitos de criminalização da contrafação e utilização através do art. 267.º do CP na versão anterior à Lei n.º 79/2021 resultava da existência de uma certa proximidade entre a moeda e os cartões de crédito, que são uma forma de "dinheiro de plástico" (cfr. acórdãos da RL de 30/06/2011 e 27/10/2020), sendo a danosidade social da contrafação de um cartão de crédito – que acaba por funcionar como o dinheiro, *maxime* no que tange ao pagamento de bens e serviços –similar à danosidade da contrafação de moeda. Contudo, tal como os cartões de crédito, os cartões de débito também podem ser vistos como uma forma de "dinheiro de plástico" e, além disso, possuem muitas das funções do cartão de crédito como as funções de levantamento de dinheiro, transferência ou pagamento, ainda que – diversamente do cartão de crédito – dependendo da existência de dinheiro na conta a que o cartão de débito está associado. E, por isso, justificar-se-ia também a equiparação dos cartões de débito à moeda para efeitos de punição, o que, a nosso ver, mal, não acontecia, sendo que, para a vítima, as consequências da utilização de um cartão de crédito contrafeito seriam praticamente equivalentes às consequências da utilização de um cartão de débito contrafeito (contra, concordando com a não inclusão do cartão de débito na equiparação prevista no art. 267.º do CP na versão anterior à Lei n.º 79/2021, ALMEIDA COSTA, *Idem*, p. 812). No entanto, como referimos no texto, a questão foi ultrapassada – e de forma correta – pela Lei n.º 79/2021.

[50] No mesmo sentido, PROCURADORIA-GERAL DA REPÚBLICA, Nota Prática n.º 24/2021, pp. 5 e 8-9.

[51] Cfr. art. 262.º, n.º 1, do CP.

abarca as criptomoedas, bem como as moedas virtuais que venham a ser emitidas por bancos centrais ou por outras autoridades públicas[52].

O art. 3.º-A (bem como o art. 3.º-F, al. b)) da Lei n.º 109/2009 constituem a transposição dos arts. 5.º, al. b), e 8.º da Diretiva 2019/713/UE, cujas imposições são observadas pelo legislador português.

O bem jurídico tutelado por esta incriminação é a intangibilidade dos sistemas e meios de pagamento diversos do numerário, incluindo a sua segurança e credibilidade (que corresponde ao bem jurídico integridade ou intangibilidade do sistema monetário legal, incluindo a segurança e a credibilidade do tráfego monetário no caso do papel-moeda e da moeda metálica, bem como das realidades equiparadas à moeda no art. 267.º do CP[53]).

O crime de contrafação de cartões ou outros dispositivos de pagamento é um crime de perigo abstrato (quanto ao grau de lesão do bem jurídico) e de resultado (quanto à modalidade de consumação do ataque ao bem jurídico), pois a lei não exige que o bem jurídico seja efetivamente colocado em perigo, limitando-se o legislador a presumir (e bem) que tais condutas são passíveis de constituir um perigo para a intangibilidade dos sistemas e meios de pagamento diversos do numerário, incluindo a sua segurança e credibilidade, mas, por outro lado, a conduta do agente gera uma modificação do mundo exterior (i.e., ocorre um evento espácio-temporalmente destacado da ação).

No que diz respeito ao tipo objetivo do crime na sua forma simples, a conduta típica consiste em introduzir, modificar, apagar, suprimir ou interferir, por qualquer outro modo, num tratamento informático de dados[54] registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a um sistema ou meio de pagamento, produzindo cartões de pagamento ou dispositivos, corpóreos ou incorpóreos, que permitam o acesso a um sistema ou meio de pagamento não genuínos, ou seja, a lei exige a prática de atos de falsificação material de um instrumento ou meio de pagamento[55]. Além disso, dado que estamos perante um crime de resultado, de acordo com a teoria da adequação, que o legislador adotou no art. 10.º, n.º 1, do CP, o ato concretamente adotado pelo agente terá de ser apto a manipular os dados informáticos ou a interferir no seu tratamento. Assim, fazendo um paralelismo com os crimes de falsificação de moeda, está em causa uma conduta análoga à conduta de contrafação de moeda (p. e p. pelo art. 262.º, n.º 1 do CP).

Uma conduta subsumível ao crime de contrafação de cartões ou outros dispositivos de pagamento é o carding[56], nos casos em que consista na manipulação

---

[52] Cfr. considerando 10 da Diretiva 2019/713/UE.

[53] Relativamente ao bem jurídico protegido pelas incriminações previstas nos arts. 262.º e ss. do CP, *vide* PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, pp. 1019, 1021, 1022, 1023 e 1024, e ALMEIDA COSTA, "Antes do Art. 262º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, pp. 748 e ss.

[54] Relativamente aos atos de introduzir, modificar, apagar, suprimir ou interferir, por qualquer outro modo, num tratamento informático de dados informáticos, *vide* DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 52-53.

[55] Como é salientado no Acórdão da RE de 22/02/2022.

[56] O *carding* consiste numa técnica de obtenção e manipulação de dados contidos na face ou nas bandas magnéticas de cartões de crédito, de débito ou de comunicações eletrónicas, bem como na

de dados contidos em bandas magnéticas de cartões de crédito ou de débito ou na implementação de dados ou de elementos de identificação em suportes técnicos relativos a sistemas ou meios de pagamento diversos do numerário.

Passando ao tipo subjetivo, o crime de contrafação de cartões ou outros dispositivos de pagamento apenas é punível a título de dolo, não sendo puníveis as condutas meramente negligentes[57], podendo a conduta do agente revestir-se de qualquer das modalidades de dolo previstas no art. 14.º do CP (direto, necessário ou eventual). No entanto, o legislador exige, para além do dolo relativamente aos elementos objetivos do tipo, um dolo específico, que consiste na intenção de provocar engano nas relações jurídicas, sendo, por isso, um crime de resultado cortado ou de intenção (Absichtsdelikte)[58].

A lei também prevê uma forma qualificada do crime de contrafação de cartões ou outros dispositivos de pagamento no art. 3.º-F, al. b), da Lei n.º 109/2009[59], consistindo a circunstância modificativa agravante na qualidade de funcionário do agente e em o crime ser cometido no exercício dessas funções. Não contendo a Lei n.º 109/2009 um conceito de funcionário, haverá que recorrer ao conceito de funcionário previsto no CP, devendo o art. 3.º-F, al. b), ser conjugado com o art. 386.º, n.ºs 1 e 2, do CP (dado que as pessoas referidas no n.º 3 apenas são consideradas funcionário para efeitos dos crimes p. e p. pelos arts. 335.º e 372.º a 374.º do CP)[60].

O crime de contrafação de cartões ou outros dispositivos de pagamento também pode ser cometido por omissão sempre que recair sobre o agente um dever de garante[61], no sentido de evitar a introdução, modificação, apagamento ou supressão dos dados informáticos registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a um sistema ou meio de pagamento ou a interferência, de qualquer outra forma, no seu tratamento, e, tendo condições para o fazer, não adotar as providências adequadas para tentar evitá-lo (cfr. art. 10.º, n.ºs 1 e 2, do CP).

Na medida em que esta incriminação tutela um bem jurídico supraindividual (o que tem repercussões ao nível do consentimento[62]), à semelhança do que sucede com o crime de contrafação de moeda p. e p. pelo art. 262.º do CP, são aplicáveis ao crime de contrafação de cartões ou outros dispositivos de pagamento as regras gerais das causas de justificação e de exclusão da culpa da Parte Geral do CP em tudo o que se refiram a tipos de crime que tutelem bens jurídicos de natureza supraindividual.

---

implementação de dados ou de elementos de identificação noutros suportes técnicos (cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 58).

[57] Cfr. art. 3.º-A da Lei n.º 109/2009, conjugado com o art. 13.º do CP.

[58] Os crimes de resultado cortado ou de intenção (*Absichtsdelikte*) são os crimes em que o tipo legal exige, para além do dolo do tipo, a intenção de produção de um resultado que não integra o tipo de ilícito (cfr. DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, p. 246).

[59] Para o qual vale o que referimos quanto ao tipo objetivo e subjetivo do crime de contrafação de cartões ou outros dispositivos de pagamento na sua forma simples.

[60] Cfr., embora relativamente ao crime de falsidade informática, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 73.

[61] Sobre as fontes do dever de garante, *vide* DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, pp. 686 e ss.

[62] Cfr. DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, pp. 432-433.

Dado que a lei não exige a apresentação de queixa nem a dedução de acusação particular, estamos perante um crime público, pelo que basta que o MP tenha conhecimento do eventual cometimento da infração para, ao abrigo dos ditames do princípio da oficialidade, instaurar o competente inquérito, nos termos dos arts. 241.º e 262.º, n.º 2, do CPP.

Não existem especificidades ao nível da comparticipação criminosa, podendo o crime de contrafação de cartões ou outros dispositivos de pagamento ser cometido a título de autoria material, autoria mediata, coautoria, instigação ou cumplicidade (moral ou material) nos termos gerais dos arts. 26.º e 27.º do CP. Também é aplicável o disposto no art. 28.º do CP quanto ao crime de contrafação de cartões ou outros dispositivos de pagamento na forma qualificada (p. e p. pelo art. 3.º-F, al. b), da Lei n.º 109/2009).

Atentas as molduras penais previstas nos arts. 3.º-A e 3.º-F, al. b), da Lei n.º 109/2009 e o disposto no art. 23.º, n.º 1, do CP, a tentativa é punível.

Por fim, quanto ao concurso de infrações, cumpre referir que, em face das modificações introduzidas pela Lei n.º 79/2021 nos arts. 3.º, n.º 2, da Lei n.º 109/2009 e 267.º, n.º 1, al. c), do CP e da introdução do crime de contrafação de cartões ou outros dispositivos de pagamento na nossa ordem jurídica, não existe qualquer sobreposição entre o âmbito de aplicação destas incriminações, atenta a diversidade dos objetos da ação de cada uma delas. Por isso, se estiver em causa a prática de factos subsumíveis a mais de um desses tipos de crime, tratar-se-á de concurso efetivo.

Relativamente ao concurso entre o crime de contrafação de cartões ou outros dispositivos de pagamento e os atos preparatórios da contrafação (p. e p. pelo art. 3.º-D da Lei n.º 109/2009), estando em causa, neste último tipo de crime, a prática de atos que, do ponto de vista estrutural, constituem atos preparatórios do crime de contrafação de cartões ou outros dispositivos de pagamento, existe uma relação de concurso aparente, sendo o crime de crime de atos preparatórios da contrafação consumido (consunção pura) pelo crime de contrafação de cartões ou outros dispositivos de pagamento[63] e funcionando os atos preparatórios como circunstância (agravante) a valorar em sede de determinação da medida da pena (cfr. art. 71.º, n.º 2, do CP).

No que concerne ao concurso entre o crime de contrafação de cartões ou outros dispositivos de pagamento e o crime de burla (p. e p. pelos arts. 217.º e ss. do CP), existe uma relação de concurso efetivo, atenta a diferença dos bens jurídicos tutelados por ambas as incriminações (intangibilidade dos sistemas e meios de pagamento diversos do numerário, incluindo a sua segurança e credibilidade vs. o património, nos crimes de burla[64]), à semelhança do que sucede entre os crimes de contrafação de

[63] À semelhança do que sucede, ao nível dos crimes de falsificação de moeda, entre o crime de contrafação de moeda (p. e p. pelo art. 262.º do CP) e os atos preparatórios (p. e p. pelo art. 271.º do CP) (cfr. PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, p. 1034, e DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, p. 730).

[64] Cfr., por todos, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, pp. 916, 923, 925, 27, 930 e 933.

moeda e o crime de burla[65] ou o crime de falsificação e contrafação de documento (p. e p. pelos arts. 256.º e 257.º do CP) e o crime de burla[66].

A situação do agente que leva a cabo a contrafação de cartões ou de outros dispositivos de pagamento e, posteriormente utiliza os mesmos será analisada infra quando analisarmos o crime de uso de cartões ou outros dispositivos de pagamento contrafeitos.

5. O novo crime de uso de cartões ou outros dispositivos de pagamento contrafeitos (artigo 3.º-B da Lei n.º 109/2009)

Dispõe o art. 3.º-B da Lei n.º 109/2009:

«1 - Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar cartão de pagamento contrafeito, ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito, é punido com pena de prisão de 1 a 5 anos.

2 - As ações descritas no número anterior são punidas com pena de prisão de 2 a 8 anos se o prejuízo ou o benefício for de valor consideravelmente elevado.

3 - As ações descritas no n.º 1 são punidas com pena de prisão de 3 a 12 anos se o agente as praticar de concerto com o agente dos factos descritos no artigo 3.º-A.».

No caso da conduta prevista no n.º 1 do art. 3.º-B, a pena passará a ser entre 2 e 5 anos de prisão quando o crime for cometido por funcionário no exercício das suas funções (cfr. art. 3.º-F, al. a))[67]. Diversamente, caso das condutas previstas nos n.ºs 2 e 3, a circunstância de o crime ser cometido por funcionário no exercício das suas funções apenas releva como circunstância (agravante), que deverá ser considerada em sede de determinação da medida concreta da pena (cfr. art. 71.º, n.º 2, do CP)[68].

A consagração legal do crime de uso de cartões ou outros dispositivos de pagamento contrafeitos foi acompanhada pela supressão da referência à utilização de "documento produzido a partir de dados informáticos registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento usar e que foram objeto de introdução, modificação, apagamento ou supressão ou cujo tratamento informático foi alvo de interferência por qualquer outra forma" no art. 3.º, n.º 3, 2.ª parte, da Lei n.º 109/2009.

Além dos cartões de crédito e de débito, o art. 3.º-B da Lei n.º 109/2009 inclui todos os demais sistemas e meios eletrónicos de pagamento (obviamente diversos do numerário), incluindo a moeda virtual (cfr. art. 3.º-G), valendo aqui mutatis mutandis o

---

[65] Cfr. Acórdão do STJ de 04/10/2007 e, à luz do Direito alemão, STREE/STERNBERG-LIEBEN, "§146", *in* Schönke/Schröder Strafgesetzbuch Kommentar, 26.ª Edição, P. 1307, e LACKNER/KÜHL, Strafgesetzbuch mit Erläuterungen, 24.ª Edição, p. 606; contra, ALMEIDA COSTA, "Art. 262º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, pp. 786 e ss.

[66] Cfr. Assentos n.ºs 3/92 e 8/2000 e AFJ n.º 10/2013; contra, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, pp. 1008-1009, e HELENA MONIZ, "Art. 256º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, p. 690.

[67] As penas abstratas previstas nos arts. 3.º-B e 3.º-F, al. a) (no que tange à conduta prevista no art. 3.º-B, n.º 1) observam a imposição do art. 9.º, n.º 2, da Diretiva 2019/713/UE.

[68] Cfr. art. 3.º-F, al. a), *a contrario sensu*, da Lei n.º 109/2009.

que referimos quanto ao crime de contrafação de cartões ou outros dispositivos de pagamento.

O art. 3.º-B (bem como o art. 3.º-F, al. a), na parte em que se refere à conduta prevista no art. 3.º-B, n.º 1) da Lei n.º 109/2009 constituem a transposição dos arts. 3.º, al. b), e 8.º da Diretiva 2019/713/UE, cujas imposições são observadas pelo legislador português.

O bem jurídico tutelado por esta incriminação é a intangibilidade dos sistemas e meios de pagamento diversos do numerário, incluindo a sua segurança e credibilidade.

O crime de uso de cartões ou outros dispositivos de pagamento contrafeitos é um crime de dano (quanto ao grau de lesão do bem jurídico) e de mera atividade (quanto à modalidade de consumação do ataque ao bem jurídico), pois ocorre uma utilização efetiva de cartões ou de outros dispositivos de pagamento contrafeitos, utilização essa que atinge efetivamente a intangibilidade daquele sistema ou meio de pagamento em concreto, incluindo a sua segurança e credibilidade, mas, por outro lado, a conduta do agente não gera qualquer modificação do mundo exterior (i.e., não se verifica qualquer evento espácio-temporalmente destacado da ação).

No que diz respeito ao tipo objetivo, no caso do crime de uso de cartões ou outros dispositivos de pagamento contrafeitos na sua forma simples (prevista no n.º 1 do art. 3.º-B), a conduta típica consiste na utilização, por qualquer modo, de um cartão de pagamento contrafeito ou de qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito. Assim, fazendo um paralelismo com os crimes de falsificação de moeda, está em causa uma conduta análoga à conduta do crime de passagem de moeda falsa (p. e p. pelo art. 265.º do CP).

Passando ao tipo subjetivo, o crime de uso de cartões ou outros dispositivos de pagamento contrafeitos apenas é punível a título de dolo, não sendo puníveis as condutas meramente negligentes[69], podendo a conduta do agente revestir-se de qualquer das modalidades de dolo previstas no art. 14.º do CP (direto, necessário ou eventual). No entanto, o legislador exige, para além do dolo relativamente aos elementos objetivos do tipo, um dolo específico, que consiste na intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, sendo, por isso, um crime de resultado cortado ou de intenção (Absichtsdelikte), tal como vimos quanto ao crime de contrafação de cartões ou outros dispositivos de pagamento.

A intenção de causar um prejuízo a outrem ou de obter um benefício ilegítimo consiste em o agente, ao utilizar cartão de pagamento contrafeito ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito, agir com intenção de, por via dessa utilização, causar um prejuízo – que pode ser patrimonial (v.g., levar à realização de um pagamento indevido) ou não patrimonial (v.g., prejudicar o bom nome) – a outra pessoa (física ou jurídica) ou obter (para si ou para outra pessoa, física ou jurídica) um benefício a que não tem direito. Embora a lei nada refira a este respeito, parece-nos que, tendo em conta aquilo que é utilizado pelo agente (cartão ou outro dispositivo de pagamento contrafeito), dificilmente o benefício visado poderá deixar de ser um benefício patrimonial, que poderá consistir na obtenção de um incremento patrimonial (v.g., receber uma quantia em dinheiro a que não tenha direito) ou na evitação de um decréscimo patrimonial

[69] Cfr. art. 3.º-B da Lei n.º 109/2009, conjugado com o art. 13.º do CP.

(v.g., conseguir a extinção de uma dívida sem que ocorra qualquer diminuição no património do agente ou do terceiro que o agente pretende beneficiar). Na medida em que a obtenção de um benefício ilegítimo não integra o tipo objetivo, basta que o agente atue com essa intenção, não tendo de ser efetivamente obtido um benefício ilegítimo, que, a ter lugar, funcionará como circunstância (agravante) que deverá ser considerada em sede de determinação da medida concreta da pena (cfr. art. 71.º, n.º 2, do CP)[70].

A lei também consagra uma forma qualificada do crime de uso de cartões ou outros dispositivos de pagamento contrafeitos[71], prevendo três circunstâncias modificativas agravantes.

A primeira dessas circunstâncias modificativas agravantes (prevista no art. 3.º-F, al. a)), consiste em o crime ser cometido por funcionário no exercício das suas funções. Não contendo a Lei n.º 109/2009 um conceito de funcionário, haverá que recorrer ao conceito de funcionário previsto no CP, devendo o art. 3.º-F, al. a), ser conjugado com o art. 386.º, n.ºs 1 e 2, do CP (dado que as pessoas referidas no n.º 3 apenas são consideradas funcionário para efeitos dos crimes p. e p. pelos arts. 335.º e 372.º a 374.º do CP)[72].

A segunda circunstância modificativa agravante (prevista no art. 3.º-B, n.º 2), consiste em o prejuízo causado ou o benefício obtido serem de valor consideravelmente elevado. Na medida em que a Lei n.º 109/2009 não contém qualquer definição de valor concretamente elevado, resta recorrer ao art. 202.º, al. b), do CP, nos termos do qual o valor consideravelmente elevado é «aquele que exceder 200 unidades de conta avaliadas no momento da prática do facto» (o que, na atualidade, significa que o valor do prejuízo causado ou do benefício obtido terá de ser superior a €20.400,00).

Por fim, a terceira circunstância modificativa agravante (prevista no art. 3.º-B, n.º 3), consiste em o agente utilizar o cartão de pagamento contrafeito ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito em concerto, ou seja, mancomunado com o agente que levara a cabo a contrafação desse cartão ou dispositivo[73], o que configura uma incriminação especial de uma forma de coautoria[74]. A finalidade desta circunstância modificativa agravante passa por punir de um modo mais grave as formas organizadas de prática desta atividade criminosa, em que, de uma maneira concertada e organizada, as organizações criminosas (incluindo as associações criminosas) e/ou

---

[70] Cfr., embora relativamente ao crime de falsidade informática, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 74.

[71] Para o qual vale o que referimos quanto ao tipo objetivo e subjetivo do crime de uso de cartões ou outros dispositivos de pagamento contrafeitos na sua forma simples.

[72] Cfr., embora relativamente ao crime de falsidade informática, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 73.

[73] Trata-se de uma conduta similar à conduta do crime de passagem de moeda falsa em concerto com o falsificador (p. e p. pelo art. 264.º do CP) no âmbito dos crimes de falsificação de moeda.

Questão diversa, que será analisada infra, é a de saber a que título deverá ser punido o agente que é, simultaneamente, a agente do ato de contrafação e do ato de utilização do cartão de pagamento contrafeito ou de outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito.

[74] Cfr., embora relativamente ao crime de passagem de moeda falsa em concerto com o falsificador (p. e p. pelo art. 264.º do CP), PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, p. 1022, e ALMEIDA COSTA, "Art. 264º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, p. 799.

terroristas[75] falsificam dados de cartões ou outros dispositivos de pagamento para depois os utilizarem de forma fraudulenta[76].

Tratando-se de um crime de mera atividade, o crime de uso de cartões ou outros dispositivos de pagamento contrafeitos não pode ser cometido por omissão, por equiparação da omissão à ação, nos termos do art. 10.º, n.ºs 1 e 2, do CP.

Na medida em que esta incriminação tutela um bem jurídico supraindividual (o que tem repercussões ao nível do consentimento[77]), à semelhança do que sucede com os crimes de passagem de moeda falsa em concerto com o falsificador e de passagem de moeda falsa (p. e p. pelos arts. 264.º e 265.º do CP, respetivamente), são aplicáveis as regras gerais das causas de justificação e de exclusão da culpa da Parte Geral do CP em tudo o que se refiram a tipos de crime que tutelem bens jurídicos que não sejam de natureza individual.

Dado que a lei não exige a apresentação de queixa nem a dedução de acusação particular, estamos perante um crime público, pelo que basta que o MP tenha conhecimento do eventual cometimento da infração para, ao abrigo dos ditames do princípio da oficialidade, instaurar o competente inquérito, nos termos dos arts. 241.º e 262.º, n.º 2, do CPP.

No caso das condutas previstas nos arts. 3.º-B, n.ºs 1 e 2, e 3.º-F, al. a) (na parte em que se refere à conduta prevista no art. 3.º-B, n.º 1), não existem especificidades ao nível da comparticipação criminosa, podendo o crime de uso de cartões ou outros dispositivos de pagamento contrafeitos ser cometido a título de autoria material, autoria mediata, coautoria, instigação ou cumplicidade (moral ou material) nos termos gerais dos arts. 26.º e 27.º do CP. Também é aplicável o disposto no art. 28.º do CP quanto ao crime de uso de cartões ou outros dispositivos de pagamento contrafeitos na forma qualificada, p. e p. pelo art. 3.º-F, al. a), da Lei n.º 109/2009; além disso, no caso da conduta prevista no art. 3.º-B, n.º 2, ainda que o cometimento do crime por funcionário no exercício das suas funções apenas releve como circunstância (agravante) para efeitos de determinação da pena concreta (como vimos), nada impede, por maioria de razão[78] a aplicação do art. 28.º do CP para efeitos de consideração da qualidade de funcionário e do facto de o crime ser cometido no exercício das suas funções ao nível da determinação da pena concreta.

Relativamente à conduta prevista no art. 3.º-B, nº 3, como referimos, trata-se de uma incriminação especial de uma forma de coautoria, o que pode suscitar dúvidas sobre se tal não terá repercussões ao nível da comparticipação criminosa. No entanto, parece-nos que não terá, visto que, independentemente da atuação concertada com

---

[75] Sobre estes conceitos, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 98 (organização criminosa *stricto sensu*), 130-131 (associação criminosa) e 171 (terrorismo e organização terrorista).

[76] Cfr. PROCURADORIA-GERAL DA REPÚBLICA, Nota Prática n.º 24/2021, p. 9.

[77] Cfr. DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, pp. 432-433.

[78] Pois, se tal norma permite a punição do *extraneus* em casos em que a mesma não teria lugar por o agente não possuir a qualidade ou relação especiais exigidas pela norma incriminadora ou a punição por um crime mais grave nos casos em que a punição, por falta dessa qualidade ou relação especiais, teria lugar por um crime menos grave, por maioria de razão, também permite a comunicação dessa qualidade ou relação especiais meramente para efeitos de determinação da pena concreta. Trata-se de uma situação de interpretação extensiva, que, diversamente, da analogia, pode ser utilizada para efeitos de fundar ou agravar a responsabilidade penal (cfr., bem como quanto à diferença entre analogia e interpretação extensiva, DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, pp. 138 e ss.).

o agente que levou a cabo a contrafação, o uso de cartões ou outros dispositivos de pagamento contrafeitos pode ser realizado conjuntamente por vários agentes no âmbito de um plano criminoso conjunto (o que configura uma situação de coautoria) e, ao mesmo tempo, em articulação com o agente dos atos de contrafação (ao ponto de, no caso de os cartões ou dispositivos terem sido alvo de contrafação por parte de uma organização criminosa lato sensu[79], a atuação dos indivíduos que fazem uso dos mesmos de forma concertada com a organização constituir uma forma de "contiguidade"[80], sendo os mesmos punidos também enquanto apoiantes da organização[81]). E, por isso, também nos casos subsumíveis ao art. 3.º-B, n.º 3, o crime de uso de cartões ou outros dispositivos de pagamento contrafeitos pode ser cometido a título de qualquer das formas de comparticipação criminosa previstas nos arts. 26.º e 27.º do CP, normas que são aplicáveis também quanto à conduta prevista no art. 3.º-B, n.º 3, que, a este nível, não apresenta quaisquer especificidades. Relativamente à aplicabilidade do art. 28.º do CP a esta conduta, vale o que referimos quanto à aplicabilidade dessa norma à conduta prevista no art. 3.º-B, n.º 2, pelo que a prática do crime por funcionário no exercício das suas funções pode ser valorada enquanto circunstância agravante em sede de determinação da pena concreta.

Atentas as molduras penais previstas nos arts. 3.º-B e 3.º-F, al. a), da Lei n.º 109/2009 e o disposto no art. 23.º, n.º 1, do CP, a tentativa é punível.

Por fim, suscitam-se algumas situações de concurso (efetivo ou aparente) de infrações.

A primeira situação cuja abordagem se justifica (de forma obviamente sucinta) é aquela em que a pessoa que utiliza o cartão ou outro dispositivo de pagamento contrafeitos é a mesma pessoa que procedera à sua contrafação. Em tais situações, consideramos que existe concurso aparente, devendo operar-se um paralelismo com o entendimento da Doutrina no que tange ao crime de contrafação de moeda (p. e p. pelo art. 262.º do CP) e ao crime de passagem de moeda falsa (p. e p. pelo art. 265.º do CP) (em que o crime de contrafação de moeda consome crime de passagem de moeda falsa, por consunção impura)[82], sendo o agente punido pela prática do crime de contrafação de cartões ou outros dispositivos de pagamento e funcionando a conduta "adicional" de utilização do cartão ou outro dispositivo de pagamento

---

[79] O que inclui a organização criminosa *stricto sensu*, a associação criminosa e a organização terrorista.

[80] Nos termos dos arts. 299.º, n.º 2, do CP (crime de associação criminosa) ou 2.º, n.º 2, da Lei n.º 52/2003, de 22 de agosto (crime de organizações terroristas), consoante o caso. Sobre o conceito de apoiante da organização criminosa e a distinção entre apoiante e angariador, *vide* FIGUEIREDO DIAS, "Art. 299º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, pp. 1167-1168, LENCKNER, "§129", *in* Schönke/Schröder Strafgesetzbuch Kommentar, 26.ª Edição, pp. 1207-1208, e PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, p. 1114.

[81] Sobre o conceito e as características da "contiguidade" à organização criminosa (*lato sensu*), *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 185 e ss.

[82] Cfr. GERMANO MARQUES DA SILVA, Direito Penal Português, Introdução e Teoria da Lei Penal, p. 295, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, p. 1020, DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, p. 731, e Acórdão do STJ de 02/11/1988; contra, entendendo que o crime de passagem de moeda falsa consome, tanto o crime de contrafação de moeda como os atos preparatórios (p. e p. pelo art. 271.º do CP), ALMEIDA COSTA, "Art. 262º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, p. 786.

Embora o crime de passagem de moeda falsa seja o crime-fim e o crime de contrafação de moeda seja o crime-meio, o agente será punido pelo crime-meio, pois possui uma moldura penal mais elevada e, por isso, a punição pelo crime-fim significaria um défice na proteção do bem jurídico no caso concreto.

contrafeitos como circunstância (agravante), que deverá ser considerada em sede de determinação da medida concreta da pena (cfr. art. 71.º, n.º 2, do CP).

A segunda situação é a relação com os crimes de passagem de moeda falsa (p. e p. pelos arts. 264.º e 265.º do CP) e de falsidade informática (no caso da conduta prevista no art. 3.º, n.º 3, 2.ª parte, da Lei n.º 109/2009), em que, em face das modificações introduzidas pela Lei n.º 79/2021 no art. 3.º, n.º 3, da Lei n.º 109/2009 e no art. 267.º, n.º 1, al. c), do CP e da introdução do crime de uso de cartões ou outros dispositivos de pagamento contrafeitos na nossa ordem jurídica, não existe qualquer sobreposição entre o âmbito de aplicação destas incriminações, atenta a diversidade dos objetos da ação de cada uma delas. Por isso, se estiver em causa a prática de factos subsumíveis a mais de um desses tipos de crime, tratar-se-á de concurso efetivo.

A terceira situação tem a ver com a relação com o crime de abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento (p. e p. pelo art. 225.º do CP). No que tange ao abuso de cartão de garantia, existindo diversidade quanto ao objeto da ação, é aplicável o que referimos quanto à relação com os crimes de passagem de moeda falsa e de falsidade informática. E o mesmo sucede ao abuso de cartão, dispositivo ou dados de pagamento[83], uma vez que também existe diversidade quanto ao objeto da ação, pois, no art. 3.º-B da Lei n.º 109/2009, está em causa a utilização de meios ou dados de pagamento contrafeitos, ao passo que, no art. 225.º do CP, está em causa a utilização abusiva (por ilegítima ou não autorizada) de meios de pagamento genuínos[84].

A quarta situação consiste na relação com o crime de burla (p. e p. pelos arts. 217.º e ss. do CP), em que, atenta a diferença dos bens jurídicos tutelados por ambas as incriminações (intangibilidade dos sistemas e meios de pagamento diversos do numerário, incluindo a sua segurança e credibilidade vs. o património, nos crimes de burla[85]), existe uma relação de concurso efetivo, à semelhança do que sucede entre o crime de passagem de moeda falsa e o crime de burla[86].

E, por último, entre o crime de uso de cartões ou outros dispositivos de pagamento contrafeitos e o crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos (p. e p. pelo art. 3.º-C da Lei n.º 109/2009), quando cometidos pelo mesmo agente, existe concurso aparente, sendo o crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos consumido pelo crime de uso de cartões ou outros dispositivos de pagamento contrafeitos, à semelhança do que ocorre

---

[83] Que consiste no uso, com intenção de obter enriquecimento ilegítimo, de cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou a meio de pagamento ou de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou a meio de pagamento, determinando o depósito, a transferência, o levantamento ou, por qualquer outra forma, o pagamento de moeda, incluindo a escritural, a eletrónica ou a virtual, e causar, desse modo, prejuízo patrimonial a outra pessoa (cfr. art. 225.º, n.º 1, als. b) a d), do CP).

[84] Cfr. PROCURADORIA-GERAL DA REPÚBLICA, Nota Prática n.º 24/2021, p. 9. No fundo, o que está em causa no art. 225.º do CP são condutas de "apropriação ilegítima", definida no considerando 15 da Diretiva 2019/713/UE, como «*a utilização sem direito a tal, com conhecimento de causa, em benefício próprio ou de terceiro, de um instrumento de pagamento não corpóreo que não em numerário por uma pessoa a quem esse instrumento tenha sido confiado*».

[85] Cfr., por todos, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, pp. 916, 923, 925, 27, 930 e 933.

[86] Cfr. PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, p. 1024, Acórdão do STJ de 13/10/2004; contra, ALMEIDA COSTA, "Art. 262º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, pp. 786 e ss.

entre o crime de aquisição de moeda falsa para ser posta em circulação (p. e p. pelo art. 266.º do CP) e o crime de passagem de moeda falsa (p. e p. pelo art. 265.º do CP) no âmbito dos crimes de falsificação de moeda[87]. No que concerne ao crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático (p. e p. pelo art. 3.º-E da mesma Lei), na medida em que, como veremos, estão aí em causa cartões e dispositivos genuínos (mas que foram obtidos através da prática de crime informático), a ulterior utilização (abusiva) dos mesmos constitui a prática do crime de abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento (p. e p. pelo art. 225.º do CP) e não do crime de uso de cartões ou outros dispositivos de pagamento contrafeitos.

6. O novo crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos (artigo 3.º-C da Lei n.º 109/2009)

Nos termos do art. 3.º-C da Lei n.º 109/2009, «Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, adquirir, detiver, exportar, importar, transportar, distribuir, vender ou por qualquer outra forma transmitir ou disponibilizar cartão de pagamento contrafeito ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito, é punido com pena de prisão de 1 a 5 anos», passando a pena a ser de prisão entre 2 e 5 anos no caso de o crime ser cometido por funcionário no exercício das suas funções (cfr. art. 3.º-F, al. a))[88].

A aquisição de cartões ou outros dispositivos de pagamento contrafeitos já era punida à luz do art. 266.º do CP, embora apenas no caso de cartões de crédito (por via da sua equiparação à moeda nos termos do art. 267.º, n.º 1, al. c), do mesmo Código). Todavia, com a supressão da referida equiparação e com a introdução dos arts. 3.º-A a 3.º-G na Lei n.º 109/2009, a aquisição de cartões de crédito contrafeitos passou a ser punida à luz do art. 3.º-C desta Lei, que inclui igualmente a aquisição de cartões de débito e de quaisquer outros dispositivos que permitam o acesso a sistema ou meio de pagamento usar (incluindo a moeda virtual, como resulta do art. 3.º-G) contrafeitos, aplicando-se mutatis mutandis o que referimos quanto ao crime de contrafação de cartões ou outros dispositivos de pagamento.

O art. 3.º-C (bem como o art. 3.º-F, al. a), na parte em que se refere à conduta prevista no art. 3.º-C) da Lei n.º 109/2009 constituem a transposição dos arts. 5.º, als. c) e d), e 8.º da Diretiva 2019/713/UE, cujas imposições são observadas pelo legislador português.

O bem jurídico tutelado por esta incriminação é, também, a intangibilidade dos sistemas e meios de pagamento diversos do numerário, incluindo a sua segurança e credibilidade.

O crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos é um crime de perigo abstrato (quanto ao grau de lesão do bem jurídico) e de mera atividade (quanto à modalidade de consumação do ataque ao bem

---

[87] Cfr. PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, p. 1025, e ALMEIDA COSTA, "Art. 265º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, p. 802.

[88] As penas abstratas previstas nos arts. 3.º-C e 3.º-F, al. a) (no que tange à conduta prevista no art. 3.º-C, sendo a referência ao n.º 1 do art. 3.º-C um lapso manifesto do legislador) observam a imposição do art. 9.º, n.º 3, da Diretiva 2019/713/UE.

jurídico), pois a lei não exige que o bem jurídico seja efetivamente colocado em perigo, limitando-se o legislador a presumir (e bem) que tais condutas são passíveis de constituir um perigo para a intangibilidade dos sistemas e meios de pagamento diversos do numerário, incluindo a sua segurança e credibilidade e não ocorre qualquer modificação do mundo exterior (i.e., não se verifica qualquer evento espácio-temporalmente destacado da ação) por via da conduta do agente.

No que diz respeito ao tipo objetivo, no caso do crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos na sua forma simples (prevista no art. 3.º-C), a conduta típica consiste em adquirir por qualquer modo[89], deter, exportar, importar, transportar, distribuir, vender ou, por qualquer outra forma, transmitir ou disponibilizar[90] um cartão de pagamento contrafeito ou de qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito. Assim, fazendo um paralelismo com os crimes de falsificação de moeda, está em causa uma conduta análoga à conduta do crime de aquisição de moeda falsa para ser posta em circulação p. e p. pelo art. 266.º do CP.

Passando ao tipo subjetivo, o crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos apenas é punível a título de dolo, não sendo puníveis as condutas meramente negligentes[91], podendo a conduta do agente revestir-se de qualquer das modalidades de dolo previstas no art. 14.º do CP (direto, necessário ou eventual). No entanto, o legislador exige, para além do dolo relativamente aos elementos objetivos do tipo, um dolo específico, que consiste na intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, sendo, por isso, um crime de resultado cortado ou de intenção (Absichtsdelikte), tal como vimos quanto ao crime de uso de cartões ou outros dispositivos de pagamento contrafeitos, valendo aqui o que referimos supra quando analisámos esse tipo de crime.

A lei também prevê uma forma qualificada do crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos no art. 3.º-F, al. a), da Lei n.º 109/2009[92], consistindo a circunstância modificativa agravante na qualidade de funcionário do agente e em o crime ser cometido no exercício dessas funções. Não contendo a Lei n.º 109/2009 um conceito de funcionário, haverá que recorrer ao conceito de funcionário

---

[89] A lei não limita a aquisição à compra ou eventualmente à permuta, pelo que a aquisição inclui os casos em que ocorra a título oneroso (*v.g.*, compra, permuta, dação em cumprimento, aluguer, etc.) ou gratuito [*v.g,* doação, depósito (na ótica do depositante, que é quem adquire), empréstimo gratuito, apropriação na sequência de achamento, etc.], definitivo (*v.g.*, compra, permuta, doação, etc.) ou temporário [*v.g.*, aluguer, depósito (na ótica do depositante, que é quem adquire), empréstimo gratuito, etc.], mediante a prática de um crime [*V.g.*, furto, roubo, burla, extorsão, etc., incluindo quando o crime seja cometido por meio informático (*v.g.*, no caso de *phishing* ou *ransomware*)], ou não, por parte do adquirente, para o agente ou para um terceiro [no mesmo sentido, embora relativamente ao crime de aquisição de moeda falsa para ser posta em circulação, PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, pp. 1024-1025, e ALMEIDA COSTA, "Art. 266º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, p. 805].

[90] Relativamente aos conceitos de importar, distribuir e vender, *vide* DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 70-71. Quanto aos demais atos previstos no art. 3.º-C, exportar significa fazer sair do território nacional, transportar significa fazer transitar de um lado para o outro (incluindo no ciberespaço e não apenas no mundo físico), deter significa ter na sua posse um cartão de pagamento contrafeito ou de qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito e "por qualquer outra forma, transmitir ou disponibilizar" constitui uma cláusula geral, à qual poderão ser subsumidos outros atos não referidos no preceito, visando o legislador obstar a lacunas de punibilidade.

[91] Cfr. art. 3.º-C da Lei n.º 109/2009, conjugado com o art. 13.º do CP.

[92] Para o qual vale o que referimos quanto ao tipo objetivo e subjetivo do crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos.

previsto no CP, devendo o art. 3.º-F, al. a), ser conjugado com o art. 386.º, n.ºs 1 e 2, do CP (dado que as pessoas referidas no n.º 3 apenas são consideradas funcionário para efeitos dos crimes p. e p. pelos arts. 335.º e 372.º a 374.º do CP)[93].

Tratando-se de um crime de mera atividade, o crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos não pode ser cometido por omissão, por equiparação da omissão à ação, nos termos do art. 10.º, n.ºs 1 e 2, do CP.

Na medida em que esta incriminação tutela um bem jurídico supraindividual (o que tem repercussões ao nível do consentimento[94]), à semelhança do que sucede com o crime de aquisição de moeda falsa para ser posta em circulação (p. e p. pelo art. 266.º), são aplicáveis as regras gerais das causas de justificação e de exclusão da culpa da Parte Geral do CP em tudo o que se refiram a tipos de crime que tutelem bens jurídicos que não sejam de natureza individual.

Dado que a lei não exige a apresentação de queixa nem a dedução de acusação particular, estamos perante um crime público, pelo que basta que o MP tenha conhecimento do eventual cometimento da infração para, ao abrigo dos ditames do princípio da oficialidade, instaurar o competente inquérito, nos termos dos arts. 241.º e 262.º, n.º 2, do CPP.

Não existem especificidades ao nível da comparticipação criminosa, podendo o crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos ser cometido a título de autoria material, autoria mediata, coautoria, instigação ou cumplicidade (moral ou material) nos termos gerais dos arts. 26.º e 27.º do CP. Também é aplicável o disposto no art. 28.º do CP quanto ao crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos qualificado

Atentas as molduras penais previstas nos arts. 3.º-C e 3.º-F, al. a), da Lei n.º 109/2009 e o disposto no art. 23.º, n.º 1, do CP, a tentativa é punível.

Por fim, suscitam-se algumas situações de concurso (efetivo ou aparente) de infrações, sendo que, quanto à relação com o crime de uso de cartões ou outros dispositivos de pagamento contrafeitos, vale o que referimos supra quando analisámos esta questão.

Quanto à relação com os crimes de aquisição de moeda falsa para ser posta em circulação (p. e p. pelo art. 266.º) e de falsidade informática (no caso da conduta prevista no art. 3.º, n.º 4, da Lei n.º 109/2009, mas apenas quanto aos atos comuns ao art. 3.º, n.º 4 e ao art. 3.º-C), em face das modificações introduzidas pela Lei n.º 79/2021 no art. 3.º, n.º 2, da Lei n.º 109/2009 e no art. 267.º, n.º 1, al. c), do CP e da introdução do crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos na nossa ordem jurídica, não existe qualquer sobreposição entre o âmbito de aplicação destas incriminações, atenta a diversidade dos objetos da ação de cada uma delas. Por isso, se estiver em causa a prática de factos subsumíveis a mais de um desses tipos de crime, tratar-se-á de concurso efetivo.

Passando à relação com o crime de abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento (p. e p. pelo art. 225.º do CP), no que tange ao abuso de cartão de garantia, existindo diversidade quanto ao objeto da ação, é aplicável o que referimos quanto à relação com os crimes de aquisição de moeda falsa

---

[93] Cfr., embora relativamente ao crime de falsidade informática, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 73.

[94] Cfr. DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, pp. 432-433.

para ser posta em circulação e de falsidade informática. E o mesmo vale para o abuso de cartão, dispositivo ou dados de pagamento[95], uma vez que também existe diversidade quanto ao objeto da ação, pois, no art. 3.º-C da Lei n.º 109/2009, está em causa a aquisição (no sentido amplo que resulta do mesmo, que, ao contrário do que resulta da epígrafe, a conduta típica não se limita à aquisição) de meios ou dados de pagamento contrafeitos, ao passo que, no art. 225.º do CP, está em causa a utilização abusiva (por ilegítima ou não autorizada) de meios de pagamento genuínos[96].

E, por último, quanto à relação com o crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático (p. e p. pelo art. 3.º-E da mesma Lei), existe diversidade quanto ao objeto da ação, pois, no art. 3.º-C da Lei n.º 109/2009, está em causa a aquisição (no sentido amplo que referimos) de meios ou dados de pagamento contrafeitos, ao passo que, no art. 3.º-E, estão em causa meios ou dados de pagamento genuínos, residindo a ilicitude da conduta de aquisição na circunstância de terem sido obtidos mediante a prática de um crime informático.

7. O novo crime de atos preparatórios da contrafação (artigo 3.º-D da Lei n.º 109/2009)

Nos termos do art. 3.º-D da Lei n.º 109/2009, «Quem produzir, adquirir, importar, distribuir, vender ou detiver qualquer cartão, dispositivo, programa ou outros dados informáticos, ou quaisquer outros instrumentos, informáticos ou não, destinados à prática das ações descritas no artigo 3.º-A, é punido com pena de prisão de 1 a 5 anos», passando a pena a ser de prisão entre 2 e 5 anos no caso de o crime ser cometido por funcionário no exercício das suas funções (cfr. art. 3.º-F, al. a))[97].

Alguns dos atos preparatórios da contrafação de cartão de pagamento ou de qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento já eram punidos no art. 3.º, n.º 4, da Lei n.º 109/2009. Todavia, além da adição de novas condutas que não constavam do art. 3.º, n.º 4[98] (produzir, adquirir e deter para outros fins que não fins comerciais), a previsão da punição dos atos preparatórios da contrafação de cartões ou outros dispositivos de pagamento foi acompanhada pela supressão da referência à manipulação de dados informáticos registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento ou do seu tratamento no art. 3.º, n.º 2, da Lei n.º 109/2009.

A punição dos atos preparatórios referidos no art. 3.º-D é imposta pelo art. 7.º da Diretiva 2019/713/UE (in casu, na parte em que remete para o art. 5.º, al. b), dessa

---

[95] Que consiste no uso, com intenção de obter enriquecimento ilegítimo, de cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou a meio de pagamento ou de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou a meio de pagamento, determinando o depósito, a transferência, o levantamento ou, por qualquer outra forma, o pagamento de moeda, incluindo a escritural, a eletrónica ou a virtual, e causar, desse modo, prejuízo patrimonial a outra pessoa (cfr. art. 225.º, n.º 1, als. b) a d), do CP).

[96] Cfr. PROCURADORIA-GERAL DA REPÚBLICA, Nota Prática n.º 24/2021, p. 9.

[97] As penas abstratas previstas nos arts. 3.º-D e 3.º-F, al. a) (no que tange à conduta prevista no art. 3.º-D) observam a imposição prevista no art. 9.º, n.º 5, da Diretiva 2019/713/UE.

[98] Mas que passaram a constar na sequência das alterações introduzidas pela Lei n.º 79/2021 nesse n.º 4 do art. 3.º da Lei n.º 109/2009.

Diretiva), nos termos do qual «Os Estados-Membros devem tomar as medidas necessárias para assegurar que sejam puníveis como infrações penais a produção, a aquisição para si próprio ou para terceiro, incluindo a importação, a exportação, a venda, o transporte, a distribuição ou a disponibilização de um dispositivo ou de um instrumento, de dados informáticos ou de outros meios principalmente concebidos ou especificamente adaptados para cometer uma das infrações previstas no artigo 4.º, alíneas a) e b), no artigo 5.º, alíneas a) e b), ou no artigo 6.º, pelo menos quando esses atos forem praticados com a intenção de que esses meios sejam utilizados»[99].

Contudo, no art. 3.º-D, o legislador não consagrou todas as condutas mencionadas no art. 7.º da Diretiva, designadamente as condutas de exportar e transportar. Por isso, ainda que a conduta de exportar possa ser subsumida às condutas de vender e de distribuir e a conduta de transportar (que importa a sua detenção pelo transportador) possa ser subsumida à conduta de deter, a sua previsão expressa é sempre preferível, a fim de afastar quaisquer dúvidas na aplicação da lei; além disso, seria desejável a introdução de uma cláusula geral (v.g., "por qualquer outro meio, disponibilizar"), como sucede nos arts. 3.º, n.º 4, 4.º, n.º 3, 5.º, n.º 2, 6.º, n.º 2, e 7.º, n.º 3, da Lei n.º 109/2009. No entanto, não ocorre qualquer incumprimento na transposição da Diretiva.

O bem jurídico tutelado por esta incriminação é, também, a intangibilidade dos sistemas e meios de pagamento diversos do numerário, incluindo a sua segurança e credibilidade.

O crime de atos preparatórios da contrafação constitui um crime de perigo abstrato (quanto ao grau de lesão do bem jurídico) e de mera atividade (quanto à modalidade de consumação do ataque ao bem jurídico), pois a lei não exige que o bem jurídico seja efetivamente colocado em perigo, limitando-se o legislador a presumir (e bem) que tais condutas são passíveis de constituir um perigo para a intangibilidade dos sistemas e meios de pagamento diversos do numerário, incluindo a sua segurança e credibilidade e não ocorre qualquer modificação do mundo exterior (i.e., não se verifica qualquer evento espácio-temporalmente destacado da ação) por via da conduta do agente[100].

No que diz respeito ao tipo objetivo, no caso o crime de atos preparatórios da contrafação na sua forma simples (prevista no art. 3.º-D), a conduta típica consiste em produzir, adquirir, importar, distribuir, vender ou deter qualquer cartão, dispositivo, programa ou outros dados informáticos ou quaisquer outros instrumentos, informáticos ou não, destinados à contrafação de cartão de pagamento ou de qualquer outro

---

[99] É também de levar em conta o considerando 13 da Diretiva quando aí se diz que «A existência de medidas de direito penal efetivas e eficientes é fundamental para proteger os meios de pagamento que não em numerário contra a fraude e a contrafação. É especialmente necessária uma abordagem comum no direito penal relativamente aos elementos constitutivos da conduta criminosa que contribuem para a efetiva utilização fraudulenta dos meios de pagamento que não em numerário ou que são preparatórios relativamente a essa utilização. Condutas como a recolha e a posse de instrumentos de pagamento com intenção de cometer uma fraude através, por exemplo, de phishing (mistificação da interface), skimming (clonagem) ou do (re)direcionamento dos utilizadores de serviços de pagamento para falsos sítios Web, e respetiva distribuição (por exemplo, através da venda de informações sobre cartões de crédito na Internet) deverão portanto configurar um tipo de infração penal por direito próprio sem que seja necessária a efetiva utilização fraudulenta dos meios de pagamento que não em numerário. Tal conduta criminosa deverá, por conseguinte, abranger igualmente circunstâncias em que a posse, a aquisição ou a distribuição não conduzem necessariamente à utilização fraudulenta desses instrumentos de pagamento».

[100] Cfr., quanto ao crime de falsidade informática, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 48 e ss.

dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, valendo aqui o que referimos quanto aos conceitos de adquirir, importar, distribuir, vender e deter quando analisámos o crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos; por seu turno, produzir consiste na criação/produção de tais cartões, dispositivos, programas ou outros dados informáticos ou quaisquer outros instrumentos, (informáticos ou não)[101].

Relativamente aos dispositivos incluídos no art. 3.º-D, ainda que se refira, no art. 7.º e no considerando 16 da Diretiva 2019/713/UE, que a mesma apenas impõe a criminalização no caso de dispositivos que sejam principalmente concebidos ou especificamente adaptados para cometer as infrações referidas na Diretiva, consideramos que esta norma inclui os dispositivos concebidos exclusiva ou especificamente para a contrafação de cartões ou outros dispositivos de pagamento e também os que, não sendo exclusiva ou especificamente concebidos para tal, poderão ser utilizados para essa finalidade, sem prejuízo de, neste último caso, ser necessário provar que se destinam a ser utilizados para fins de contrafação de cartões ou outros dispositivos de pagamento, valendo aqui mutatis mutandis o que referimos supra relativamente ao crime de acesso ilegítimo (designadamente quanto ao art. 6.º, n.º 3, da Lei n.º 109/2009).

Passando ao tipo subjetivo, os atos preparatórios da contrafação apenas são puníveis a título de dolo, não sendo puníveis as condutas meramente negligentes[102], podendo a conduta do agente revestir-se de qualquer das modalidades de dolo previstas no art. 14.º do CP (direto, necessário ou eventual).

A lei também prevê uma forma qualificada do crime de atos preparatórios da contrafação no art. 3.º-F, al. a), da Lei n.º 109/2009[103], consistindo a circunstância modificativa agravante em o crime ser praticado por funcionário no exercício das suas funções. Não contendo a Lei n.º 109/2009 um conceito de funcionário, haverá que recorrer ao conceito de funcionário previsto no CP, devendo o art. 3.º-F, al. a), ser conjugado com o art. 386.º, n.ºs 1 e 2, do CP (dado que as pessoas referidas no n.º 3 apenas são consideradas funcionário para efeitos dos crimes p. e p. pelos arts. 335.º e 372.º a 374.º do CP)[104].

Tratando-se de um crime de mera atividade, o crime de atos preparatórios da contrafação não pode ser praticados por omissão, por equiparação da omissão à ação, nos termos do art. 10.º, n.ºs 1 e 2, do CP.

Na medida em que esta incriminação tutela um bem jurídico supraindividual (o que tem repercussões ao nível do consentimento[105]), à semelhança do que sucede com o crime de contrafação de moeda p. e p. pelo art. 262.º do CP, são aplicáveis as regras gerais das causas de justificação e de exclusão da culpa da Parte Geral do CP em tudo o que se refiram a tipos de crime que tutelem bens jurídicos de natureza supraindividual.

---

[101] Cfr., embora relativamente ao crime de dano relativo a programas ou outros dados informáticos, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 104.

[102] Cfr. art. 3.º-D da Lei n.º 109/2009, conjugado com o art. 13.º do CP.

[103] Para o qual vale o que referimos quanto ao tipo objetivo e subjetivo da infração na sua forma simples.

[104] Cfr., embora relativamente ao crime de falsidade informática, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 73.

[105] Cfr. DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, pp. 432-433.

Atentas as molduras penais previstas nos arts. 3.º-D e 3.º-F, al. a), da Lei n.º 109/2009 e o disposto no art. 23.º, n.º 1, do CP, a tentativa é punível[106].

Na medida em que, para que o agente seja punido pela prática infração, terá de praticar um facto típico, ilícito e culposo (e punível), para além do preenchimento dos elementos objetivos e subjetivos do tipo, não poderão verificar-se os pressupostos de qualquer causa de exclusão da ilicitude, da culpa ou da punibilidade. Contudo, uma vez que esta incriminação tutela um bem jurídico supraindividual (o que tem repercussões ao nível do consentimento[107]), são aplicáveis as regras gerais das causas de justificação e de exclusão da culpa da Parte Geral do CP em tudo o que se refiram a tipos de crime que tutelem bens jurídicos que não sejam de cariz eminentemente pessoal.

Dado que a lei não exige a apresentação de queixa nem a dedução de acusação particular, estamos perante um crime público, pelo que basta que o MP tenha conhecimento do eventual cometimento da infração para, ao abrigo dos ditames do princípio da oficialidade, instaurar o competente inquérito, nos termos dos arts. 241.º e 262.º, n.º 2, do CPP.

Não existem especificidades ao nível da comparticipação criminosa, podendo a infração ser cometida a título de autoria material, autoria mediata, coautoria, instigação ou cumplicidade (moral ou material) nos termos gerais dos arts. 26.º e 27.º do CP. Também é aplicável o disposto no art. 28.º do CP quanto à infração na sua forma qualificada.

No que concerne ao concurso de infrações, quando o mesmo agente pratique algum ou alguns os atos preparatórios da contrafação p. e p. pelo art. 3.º-D e, subsequentemente leve a cabo a contrafação de cartões ou outros dispositivos de pagamento, como referimos quando analisámos o crime de contrafação de cartões ou outros dispositivos de pagamento, existe uma relação de concurso aparente, sendo os atos preparatórios da contrafação consumidos pelo crime de contrafação de cartões ou outros dispositivos de pagamento, funcionando apenas como circunstância (agravante) a valorar em sede de determinação da medida da pena (cfr. art. 71.º, n.º 2, do CP). A punição pelos atos preparatórios da contrafação também é afastada (por subsidiariedade) nos casos de tentativa de contrafação de cartões ou outros dispositivos de pagamento, mas volta a ter lugar se o agente desistir da tentativa nos termos previstos nos arts. 24.º e 25.º do CP (consoante a situação concreta)[108]; quando a punição dos atos preparatórios da contrafação for afastada por via da tentativa de contrafação de cartões ou outros dispositivos de pagamento vale o que referimos supra quanto à sua consideração em sede de determinação da pena concreta.

---

[106] Relativamente à possibilidade de punição da tentativa no caso de condutas típicas que respeitem a atos que, do ponto de vista estrutural, são atos preparatórios de outros tipos de crime, *vide*, embora relativamente ao crime de dano relativo a programas ou outros dados informáticos, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 109-110.

[107] Cfr. DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, pp. 432-433.

[108] Cfr., embora quanto aos atos preparatórios dos crimes de falsificação de moeda, título de crédito e valor selado (p. e p. pelo art. 271.º do CP), FIGUEIREDO DIAS, Direito Penal, Parte Geral, Tomo I, 3.ª Edição, p. 1161, e ALMEIDA COSTA, "Art. 271º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, pp. 863-864.

8. O novo crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático (artigo 3.º-E da Lei n.º 109/2009)

Dispõe o art. 3.º-E da Lei n.º 109/2009:

«Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, adquirir, detiver, exportar, importar, transportar, distribuir, vender ou por qualquer outra forma transmitir ou disponibilizar:

a) Dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, que hajam sido obtidos mediante facto ilícito típico previsto nos artigos 4.º, 5.º, 6.º e 7.º;

b) Cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, que haja sido obtido mediante facto ilícito típico previsto nos artigos 4.º, 5.º, 6.º e 7.º;

é punido com pena de prisão de 1 a 5 anos».

Se o crime for cometido por funcionário no exercício das suas funções, a pena passará a ser entre 2 e 5 anos de prisão (cfr. art. 3.º-F, al. a))[109].

O crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático pune a aquisição (no sentido amplo que veremos infra) de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, de cartões de pagamento ou de qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento genuínos, residindo a ilicitude da conduta de aquisição na circunstância de terem sido obtidos mediante a prática de um crime informático (designadamente dos crimes p. e p. pelos arts. 4.º a 7.º da Lei n.º 109/2009), constituindo um caso de neocriminalização. Como referimos, o crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático distingue-se do crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos pelo facto de, no crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos, estar em causa a aquisição (no conceito amplo referido supra) de cartões ou outros dispositivos de pagamento não genuínos, residindo a ilicitude, não na sua obtenção através da prática de crimes, mas sim na sua falsidade.

A criminalização da aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático visa punir os indivíduos que se dediquem ao florescente negócio de compra e venda, por exemplo, na Dark Web, de dados de cartões bancários verdadeiros, obtidos por via de ataques informáticos[110].

O art. 3.º-E (bem como o art. 3.º-F, al. a), na parte em que se refere à conduta prevista no art. 3.º-E) da Lei n.º 109/2009 constituem a transposição dos arts. 5.º, als. a),

[109] As penas abstratas previstas nos arts. 3.º-E e 3.º-F, al. a) (no que tange à conduta prevista no art. 3.º-E) observam a imposição do art. 9.º, n.º 4, da Diretiva 2019/713/UE.

[110] Cfr. PROCURADORIA-GERAL DA REPÚBLICA, Nota Prática n.º 24/2021, p. 10.

c) e d), e 8.º da Diretiva 2019/713/UE[111], cujas imposições são observadas pelo legislador português.

O bem jurídico tutelado por esta incriminação é o património, à semelhança do que sucede com o crime de abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento (p. e p. pelo art. 225.º do CP)[112], que, como veremos, consome esta incriminação quando seja cometido na sequência do cometimento desta. Na verdade, não há aqui qualquer atentado contra intangibilidade dos sistemas e meios de pagamento diversos do numerário, incluindo a sua segurança e credibilidade, pois estão em causa cartões ou outros dispositivos de pagamento genuínos; o que existe é a prática de atos passíveis de, subsequentemente, possibilitarem a utilização abusiva desses cartões ou dispositivos genuínos e, dessa forma, lesar o património dos seus legítimos proprietários.

O crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático é um crime de perigo abstrato (quanto ao grau de lesão do bem jurídico) e de mera atividade (quanto à modalidade de consumação do ataque ao bem jurídico), pois a lei não exige que o bem jurídico seja efetivamente colocado em perigo, limitando-se o legislador a presumir (e bem) que tais condutas são passíveis de constituir um perigo para património, e não ocorre qualquer modificação do mundo exterior (i.e., não se verifica qualquer evento espácio-temporalmente destacado da ação) por via da conduta do agente.

No que diz respeito ao tipo objetivo, no caso do crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático na sua forma simples (prevista no art. 3.º-E), a conduta típica consiste em adquirir, deter, exportar, importar, transportar, distribuir, vender ou, por qualquer outra forma, transmitir ou disponibilizar[113] dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, de cartões de pagamento ou de qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento genuínos, mas obtidos mediante a prática de um crime de dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo ou interceção ilegítima. De notar que podem estar em causa quaisquer meios de pagamento, incluindo os relativos a moeda virtual (cfr. art. 3.º-G).

---

[111] A este respeito, cumpre, ainda, ter presente o considerando 15 da Diretiva, quando aí se afirma que «A presente diretiva faz referência a formas de conduta clássicas, como fraude, falsificação, furto e apropriação ilícita, que já foram delineadas pelo direito nacional antes da era digital. O âmbito alargado da presente diretiva no que diz respeito aos instrumentos de pagamento não corpóreos implica portanto a definição de formas de conduta equivalentes na esfera digital, que complementem e reforcem a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho. A obtenção ilícita de um instrumento de pagamento não corpóreo que não em numerário deverá configurar uma infração penal, pelo menos quando envolva a prática de uma das infrações referidas nos artigos 3.º a 6.º da Diretiva 2013/40/UE, ou a apropriação ilegítima de um instrumento de pagamento não corpóreo que não em numerário. Por «apropriação ilegítima», deverá entender-se a utilização sem direito a tal, com conhecimento de causa, em benefício próprio ou de terceiro, de um instrumento de pagamento não corpóreo que não em numerário por uma pessoa a quem esse instrumento tenha sido confiado. A aquisição para utilização fraudulenta de um desses instrumentos obtido de forma ilícita deverá ser punível, sem ser necessário estabelecer todos os elementos factuais da obtenção ilícita, e sem exigir uma condenação anterior ou simultânea por uma infração subjacente que tenha dado origem à obtenção ilícita».

[112] Cfr. PAULO PINTO DE ALBUQUERQUE, Comentário do Código Penal, 4.ª Edição, p. 943, e DAMIÃO DA CUNHA, "Art. 225º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, p. 375.

[113] Relativamente a estes atos, *vide* o que referimos supra quando analisámos o crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos.

Passando ao tipo subjetivo, o crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático apenas é punível a título de dolo, não sendo puníveis as condutas meramente negligentes[114], podendo a conduta do agente revestir-se de qualquer das modalidades de dolo previstas no art. 14.º do CP (direto, necessário ou eventual), incluindo o tipo subjetivo o conhecimento ou, pelo menos, a representação da possibilidade (e a conformação do agente com essa possibilidade) de que os dados informáticos, os cartões ou os outros dispositivos foram/possam ter sido obtidos mediante a prática de um dos crimes referidos no art. 3.º-E, o que será difícil de negar nos casos – como sucede frequentemente – em que o agente os tenha adquirido em páginas da Dark Web. No entanto, o legislador exige, para além do dolo relativamente aos elementos objetivos do tipo, um dolo específico, que consiste na intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, sendo, por isso, um crime de resultado cortado ou de intenção (Absichtsdelikte), tal como vimos quanto ao crime de uso de cartões ou outros dispositivos de pagamento contrafeitos, valendo aqui mutatis mutandis o que referimos supra quando analisámos esse tipo de crime.

A lei também prevê uma forma qualificada do crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático no art. 3.º-F, al. a), da Lei n.º 109/2009[115], consistindo a circunstância modificativa agravante em o crime ser praticado por funcionário no exercício das suas funções. Não contendo a Lei n.º 109/2009 um conceito de funcionário, haverá que recorrer ao conceito de funcionário previsto no CP, devendo o art. 3.º-F, al. a), ser conjugado com o art. 386.º, n.ºs 1 e 2, do CP (dado que as pessoas referidas no n.º 3 apenas são consideradas funcionário para efeitos dos crimes p. e p. pelos arts. 335.º e 372.º a 374.º do CP)[116].

Tratando-se de um crime de mera atividade, o crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático não pode ser cometido por omissão, por equiparação da omissão à ação, nos termos do art. 10.º, n.ºs 1 e 2, do CP.

São aplicáveis ao crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático as regras gerais das causas de justificação e de exclusão da culpa da Parte Geral do CP.

Dado que a lei não exige a apresentação de queixa nem a dedução de acusação particular, estamos perante um crime público, pelo que basta que o MP tenha conhecimento do eventual cometimento da infração para, ao abrigo dos ditames do princípio da oficialidade, instaurar o competente inquérito, nos termos dos arts. 241.º e 262.º, n.º 2, do CPP.

Não existem especificidades ao nível da comparticipação criminosa, podendo o crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático ser cometido a título de autoria material, autoria mediata, coautoria, instigação ou cumplicidade (moral ou material) nos termos gerais dos arts. 26.º e 27.º do CP. Também é aplicável o disposto no art. 28.º do CP quanto ao crime de aquisição de

---

[114] Cfr. art. 3.º-E da Lei n.º 109/2009, conjugado com o art. 13.º do CP.

[115] Para o qual vale o que referimos quanto ao tipo objetivo e subjetivo do crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos.

[116] Cfr., embora relativamente ao crime de falsidade informática, DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, p. 73.

cartões ou outros dispositivos de pagamento obtidos mediante crime informático qualificado

Atentas as molduras penais previstas nos arts. 3.º-C e 3.º-F, al. a), da Lei n.º 109/2009 e o disposto no art. 23.º, n.º 1, do CP, a tentativa é punível.

Por fim, suscitam-se algumas situações de concurso (efetivo ou aparente) de infrações, sendo que, quanto à relação com o crime de aquisição de cartões ou outros dispositivos de pagamento contrafeitos, vale o que referimos supra quando analisámos este tipo de crime.

No que diz respeito a uma eventual relação com o crime de uso de cartões ou outros dispositivos de pagamento contrafeitos, não existe qualquer relação, pois o uso abusivo de cartões ou outros dispositivos de pagamento genuínos (que é o que está em causa no crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático) é punido pelo art. 225.º do CP e não pelo art. 3.º-B da lei n.º 109/2009.

Quanto à relação com o crime de abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento (p. e p. pelo art. 225.º do CP), no que tange ao abuso de cartão de garantia, existindo diversidade quanto ao objeto da ação, é aplicável o que referimos quanto à relação com os crimes de aquisição de moeda falsa para ser posta em circulação e de falsidade informática. E o mesmo sucede quanto ao abuso de cartão, dispositivo ou dados de pagamento[117], uma vez que existe uma relação de concurso aparente, sendo o crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático consumido pelo crime de abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento e constituindo os atos subsumíveis ao crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático circunstâncias (agravantes), que deverão ser consideradas na determinação da pena concreta (cfr. art. 71.º, n.º 2, do CP).

Por fim, relativamente à relação com os crimes de dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo e interceção ilegítima, atenta a diversidade do bem jurídico tutelado pelo crime de aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático face aos bens jurídicos tutelados por cada um dos demais crimes[118], existe uma relação de concurso efetivo.

---

[117] Que consiste no uso, com intenção de obter enriquecimento ilegítimo, de cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou a meio de pagamento ou de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou a meio de pagamento, determinando o depósito, a transferência, o levantamento ou, por qualquer outra forma, o pagamento de moeda, incluindo a escritural, a eletrónica ou a virtual, e causar, desse modo, prejuízo patrimonial a outra pessoa (cfr. art. 225.º, n.º 1, als. b) a d), do CP).

[118] Relativamente aos bens jurídicos tutelados pelos crimes de dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo e interceção ilegítima, *vide* DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime, pp. 93-94, 125-126, 156-157 e 186-187.

9. A imposição, pela Diretiva 2019/713/UE, de um limiar mínimo da pena máxima aplicável nos casos em que os crimes sejam cometidos no contexto de uma organização criminosa é observada na Lei n.º 109/2009?

Nos termos do art. 9.º, n.º 6, da Diretiva 2019/713/UE, «Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infrações previstas nos artigos 3.º a 6.º sejam puníveis com uma pena de prisão máxima não inferior a cinco anos se forem cometidas no contexto de uma organização criminosa, na aceção da Decisão-Quadro 2008/841/JAI, independentemente da sanção prevista nessa decisão».

Além disso, diz-se, no considerando 19 da Diretiva, que «Considera-se adequado prever sanções mais severas quando uma infração é cometida no contexto de uma organização criminosa, na aceção da Decisão-Quadro 2008/841/JAI do Conselho. Os Estados-Membros não deverão ser obrigados a prever circunstâncias específicas agravantes caso o direito nacional preveja infrações penais distintas e tal possa conduzir à aplicação de sanções mais severas. (…)».

No caso das sanções previstas nos arts. 3.º-A a 3.º-F da Lei n.º 109/2009, a exigência do art. 9.º, n.º 6, da Diretiva é observada, pois o limite máximo "mínimo" das penas aplicáveis é de 5 anos.

Passando ao art. 6.º da Lei n.º 109/2009, no caso do art. 6.º, n.º 3, em que está em causa a transposição do art. 7.º da Diretiva, a imposição prevista no art. 9.º, n.º 6, não se aplica[119]. Mas o mesmo já não sucede no caso do art. 6.º, n.º 4, al. b), pois o limite máximo da pena aplicável é de 3 anos sem se prever uma pena de prisão de, pelo menos, até 5 anos no caso de o crime ser cometido no contexto de uma organização criminosa[120], o que constitui uma não transposição da Diretiva neste ponto.

10. A responsabilidade penal dos entes coletivos relativamente aos crimes previstos nos artigos 3.º-A a 3.º-F da Lei n.º 109/2009

O art. 9.º da Lei n.º 109/2009, onde se prevê a responsabilização penal dos entes coletivos relativamente à prática dos "crimes previstos na presente lei nos termos e limites do regime de responsabilização previsto no Código Penal" não sofreu qualquer modificação por via da entrada em vigor da Lei n.º 79/2021, uma vez que, pela redação que já possuía, prevê a responsabilidade penal dos entes coletivos relativamente aos crimes previstos nos arts. 3.º-A a 3.º-F e às novas condutas típicas adicionadas ao crime de acesso ilegítimo (p. e p. pelo art. 6.º da Lei n.º 109/2009).

No que diz respeito às penas referidas no art. 11.º da Diretiva 2019/713/UE, todas essas penas estão previstas nos arts. 90.º-A e ss. do CP, sendo aplicáveis aos crimes previstos na Lei n.º 109/2009 (cfr. art. 9.º desta Lei).

---

[119] Sendo que o art. 6.º, n.º 3, da Lei n.º 109/2009 observa a imposição prevista no art. 9.º, n.º 5, da Diretiva.

[120] *In casu*, uma associação criminosa, tal como prevista no art. 299.º do CP, e/ou uma organização terrorista, tal como prevista no art. 2.º da Lei n.º 52/2003, de 22 de agosto.

11. Aplicação no tempo

Na medida em que não se nos afigura que da aplicação das alterações introduzidas pela Lei n.º 79/2021 na Lei n.º 109/2009 possa resultar a aplicação de uma norma concretamente mais favorável ao agente, nos termos do arts. 29.º, n.ºs 1, 3 e 4, da CRP e 1.º e 2.º, n.º 1, do CP, o regime decorrente das alterações introduzidas pela Lei n.º 79/2021 na Lei n.º 109/2009 só são aplicáveis aos factos praticados a partir da entrada em vigor da Lei n.º 79/2021 (24/12/2021[121]).

12. Conclusões

A Lei n.º 79/2021, de 24 de novembro, transpôs para a ordem jurídica portuguesa a Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, tendo introduzido alterações em vários diplomas, entre os quais, a Lei n.º 109/2009, de 15 de setembro;

Na Lei n.º 109/2009, a Lei n.º 79/2021 introduziu modificações nos capítulos II (disposições penais materiais), III (disposições processuais) e IV (cooperação internacional);

Nas disposições penais materiais da Lei n.º 109/2009, a Lei n.º 79/2021 modificou os arts. 3.º e 6.º (que criminalizam a falsidade informática e o acesso ilegítimo) e introduziu novos tipos de crime nos arts. 3.º-A a 3.º-F (embora algumas das condutas incriminadas nesses novos tipos de crime já fossem punidas como crime na nossa ordem jurídica), assim como esclarece que a Lei n.º 109/2009 inclui os sistemas ou meios de pagamento que tenham por objeto moeda virtual (o que inclui as criptomoedas, como resulta da definição de moeda virtual constante do art. 2.º, al. d), da Diretiva 2019/713/UE);

A grande maioria das modificações introduzidas pela Lei n.º 79/2021 na Lei n.º 109/2009 observa as imposições de criminalização (arts. 5.º, 7.º, 8.º e 10.º) e de punição (arts. 9.º e 11.º) constantes da Diretiva 2019/713/UE, mas o mesmo já não sucede no que tange à não punição da conduta criminalizada no art. 6.º, n.º 4, al. b), da Lei n.º 109/2009 quando cometida no âmbito de uma associação criminosa ou organização terrorista e à não previsão de uma pena de prisão até 2 anos para a conduta de aceder ilegitimamente a um sistema informático com a finalidade de obter dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento;

O legislador aproveitou a oportunidade concedida pela transposição da Diretiva 2019/713/UE para corrigir algumas lacunas/imperfeições da Lei n.º 109/2009, designadamente algumas daquelas de que padecia o art. 3.º, n.º 4, e que havíamos recenseado na nossa obra Os crimes previstos na Lei do Cibercrime;

Todavia, apesar de, para além de apresentar outras lacunas/imperfeições/incongruências, a Lei n.º 109/2009 não cumprir algumas das imposições de criminalização e punição constantes da Diretiva **2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto,** relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho, que também recenseámos na nossa obra Os crimes previstos na Lei do Cibercrime, o

[121] Cfr. art. 21.º da Lei n.º 79/2021.

legislador não aproveitou a oportunidade concedida pela transposição da Diretiva 2019/713/UE para corrigir esses aspetos da referida Lei n.º 109/2009.

Bibliografia

Albuquerque, Paulo Pinto de – Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, 4.ª Edição, Universidade Católica Editora, Lisboa, 2021.

Costa, António Manuel de Almeida – "Antes do Art. 262º", in Comentário Conimbricense do Código Penal Parte Especial, Tomo II, pp. 737 e ss., Coimbra Editora, Coimbra, 1999.

Costa, António Manuel de Almeida – "Art. 262º", in Comentário Conimbricense do Código Penal Parte Especial, Tomo II, pp. 759 e ss., Coimbra Editora, Coimbra, 1999.

Costa, António Manuel de Almeida – "Art. 264º", in Comentário Conimbricense do Código Penal Parte Especial, Tomo II, pp. 798-799, Coimbra Editora, Coimbra, 1999.

Costa, António Manuel de Almeida – "Art. 265º", in Comentário Conimbricense do Código Penal Parte Especial, Tomo II, pp. 800 e ss., Coimbra Editora, Coimbra, 1999.

Costa, António Manuel de Almeida – "Art. 267º", in Comentário Conimbricense do Código Penal Parte Especial, Tomo II, pp. 807 e ss., Coimbra Editora, Coimbra, 1999.

Costa, António Manuel de Almeida – "Art. 271º", in Comentário Conimbricense do Código Penal Parte Especial, Tomo II, pp. 857 e ss., Coimbra Editora, Coimbra, 1999.

Cunha, José Manuel Damião da – "Art. 225º", in Comentário Conimbricense do Código Penal Parte Especial, Tomo II, pp. 373 e ss., Coimbra Editora, Coimbra, 1999.

Dias, Jorge de Figueiredo – "Art. 299º", in Comentário Conimbricense do Código Penal Parte Especial, Tomo II, pp. 1155 e ss., Coimbra Editora, Coimbra, 1999.

Dias, Jorge de Figueiredo – Direito Penal, Parte Geral, Tomo I, 3.ª Edição, Coimbra Editora, Coimbra, 2019.

Dias, Pedro Simões – "O "Hacking" enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo Direito", in Direito da Sociedade da Informação, Volume VIII, pp. 229 e ss., Coimbra Editora, Coimbra, 2009.

Lackner, Karl/Kühl, Kristian – Strafgesetzbuch mit Erläuterungen, 24.ª Edição, Verlag B.H. Beck, Munique, 2001.

Leckner, Theodor – "§129", in Schönke/Schröder Strafgesetzbuch Kommentar, 26.ª Edição, pp. 1200 e ss., Verlag C.H. Beck, Munique, 2001.

Macedo, João Carlos da Cruz Barbosa de – "Algumas considerações acerca dos crimes informáticos em Portugal", in Direito Penal Hoje, Novos desafios e novas respostas, pp. **221 e ss., Coimbra Editora, Coimbra, 2009.**

Moniz, Helena – "Art. 256º", in Comentário Conimbricense do Código Penal Parte Especial, Tomo II, pp. 674 e ss., Coimbra Editora, Coimbra, 1999.

Nunes, Duarte Rodrigues – O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, Gestlegal, Coimbra, 2019.

Nunes, Duarte Rodrigues – Os crimes previstos na Lei do Cibercrime, Gestlegal, Coimbra, 2020.

Nunes, Duarte Rodrigues – Curso de Direito Penal, Parte Geral, Tomo I, Questões fundamentais e teoria geral do crime, Gestlegal, Coimbra, 2021.

Nunes, Duarte Rodrigues – Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, Gestlegal, Coimbra, 2021.

Procuradoria-Geral da República – Nota Prática n.º 24/2021, in https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_24_novos_crimes_na_lei_cibercrime.pdf (consultado em 01/09/2022).

Rocha, Manuel António Lopes – "A lei da criminalidade informática (Lei n.º 109/01 de 17 de Agosto). Génese e técnica legislativa", in Cadernos de Ciência de Legislação, n.º 8 (Outubro-Dezembro 1993), pp. 65 e ss., Instituto Nacional da Administração, Lisboa, 1993.

Silva, Germano Marques da – Direito Penal Português, Introdução e Teoria da Lei Penal, Universidade Católica Editora, Lisboa, 2020.

Stree, Walter/Sternberg-Lieben, Detlev – "§146", in Schönke/Schröder Strafgesetzbuch Kommentar, 26.ª Edição, pp. 1301 e ss., Verlag C.H. Beck, Munique, 2001.

Verdelho, Pedro – "A nova Lei do Cibercrime", in Scientia Ivridica, Tomo LVIII (2009), pp. 717 e ss., Universidade do Minho, Braga, 2009.

Verdelho, Pedro/Bravo, Rogério/Rocha, Manuel Lopes – Leis do Cibercrime, Volume I, Centro Atlântico, Vila Nova de Famalicão, 2003.

Jurisprudência

Supremo Tribunal de Justiça

Jurisprudência fixada

Assento n.º 3/92, publicado no Diário da República, I Série, de 9 de abril de 1992.
Assento n.º 8/2000, publicado no Diário da República, I Série, de 23 de maio de 2000.
Assento n.º 10/2013, publicado no Diário da República, I Série, de 7 de outubro de 2013.

Outra jurisprudência

Acórdão de 2 de novembro de 1988 (Proc. 039680), in www.dgsi.pt
Acórdão de 13 de outubro de 2004 (Proc. 04P3210), in www.dgsi.pt
Acórdão de 4 de outubro de 2007 (Proc. 07P2309), in www.dgsi.pt

Tribunal da Relação de Évora

Acórdão de 22 de fevereiro de 2022 (Proc. 188/21.7GAVNO.E1), in www.dgsi.pt

Tribunal da Relação de Guimarães

Acórdão de 27 de outubro de 2008 (Proc. 1339/08-1), in www.dgsi.pt
Acórdão de 17 de novembro de 2008 (Proc. 2233/07), in www.alain-bensoussan.com/wp-content/uploads/2014/06/24294369.pdf
(consultado em 01/09/2022).

Tribunal da Relação de Lisboa

Acórdão de 30 de junho de 2011 (Proc. 189/09.3JASTB.L1-5), in www.dgsi.pt
Acórdão de 10 de julho de 2012 (Proc. 7876/10.1JFLSB.L1-5), in www.dgsi.pt
Acórdão de 27 de outubro de 2020 (Proc. 294/17.2JGLSB.L2 -5), in www.dgsi.pt

Data Leaks e Monitoramento de Riscos Cibernéticos: o megavazamento de dados no Brasil em 2021 e os serviços de segurança para "proteção ao crédito"

Gustavo Rabay Guerra[122]
Amanda de Castro Cavallaro[123]

RESUMO

Com o desenvolvimento tecnológico num ritmo nunca visto antes e a hiperconectividade digital cada vez mais presente no cotidiano do indivíduo, os riscos e ameaças de ataques cibernéticos se tornam cada vez mais presente, em especial em empresas que possuam um rico banco de dados, como as instituições voltadas à "proteção ao crédito". Contudo, observa-se que a busca desenfreada das empresas por informações tem se tornado, em sim um risco. O presente estudo traz como caso paradigma o megavazamento de dados da Serasa Experian, partindo desde a sua caracterização aos impactos, e por fim, às sanções, ou, no caso, a falta delas, em especial tendo em vista o advento da Lei Geral de Proteção de Dados (LGPD).

PALAVRAS-CHAVE:

Data Leak; Ciberataques; Vazamento de Dados; Serviço de Proteção ao Crédito

[122] Advogado. Professor Associado da Universidade Federal da Paraíba (UFPB). Doutor em Direito, Estado e Constituição pela Universidade de Brasília (UNB). Mestre em Direito pela Universidade Federal de Pernambuco (UFPE). Fundador da Compliance Academy e Idealizador da Legal Mind.

[123] Advogada, Consultora e Head de Privacidade e Proteção de Dados. Mestranda em Direito na Universidade Federal do Rio Grande do Sul. Pós-graduanda em Direito Empresarial na Pontifícia Católica do Rio Grande do Sul (PUC-RS). Bacharela em Direito pela Universidade Federal da Paraíba (UFPB). Analista de Dados pelo IGTI. Community Manager da Compliance Academy.

Data Leaks and Monitoring of Cyber Risks: the mega data leak in Brazil in 2021 and the services security for "protection to credit"

Gustavo Rabay Guerra
Amanda de Castro Cavallaro

ABSTRACT

Given the technological development at a pace never seen before and digital hyperconnectivity in the everyday life, the risks and threats of cyberattacks become increasingly present, especially in companies that have a rich database, such as institutions focused on "credit protection". However, it is observed that the frantic search for information by companies has become, in fact, a risk. This study brings as a paradigm case the massive data leak from Serasa Experian, starting from its characterization to the impacts, and finally, the sanctions, or in this case, the lack of them, especially in view of the advent of the Brazilian General Data Protection Law (LGPD).

KEYWORDS

Data Leak; Cyberattacks; Data Brench; Credit Protection Service

1. Primeiras linhas

Tratando-se de um fenômeno recente, a hiperconectividade digital tem gerado infinitos benefícios a todo e qualquer cidadão que passa a se utilizar da "infovia" ou da "tecnoesfera". O fato, sem a intenção de estender demasiado questões socioeconômicas de fundo, vivemos a era da expansão global das "Big Techs" e do "Big Data". Com eles, avultam os riscos cibernéticos e ameaças crescentes, como incidentes de segurança específicos que comprometem a privacidade e os dados pessoais aqui aludidos.

Além dos dados pessoais constantes em fichas de cadastro, os hábitos de consumo, as linhas de crédito e o micro comportamento dos usuários são os dados que as empresas buscam desenfreadamente para entender a jornada de consumo dos seus potenciais consumidores em um cruzamento de informações que já têm em sua própria base, construída a partir dos dados coletados de seus consumidores. Fala-se, inclusive, na ascensão de uma nova religião ou de uma nova divindade, para a qual entregamos nossas vidas – o "dataísmo", a crença absoluta na direção da sociedade a partir de dados (HARARI, 2016, pp. 321-322).

Na mesma senda, é possível falar de uma sociedade que se encontra "aprisionada" no denominado "capitalismo de vigilância" segundo o qual o fenômeno de grandes acervos informacionais ("Big Data") não é simplesmente uma ferramenta tecnológica ou uma metodologia, mas uma ditadura comportamental imposta pelas grandes corporações (ZUBOFF, 2015) - as mesmas que adquirem as informações de grandes bancos de dados sob o pretexto de tratamento legítimo para fins de "proteção de crédito".

Em 11 de janeiro de 2021, um banco de dados contendo informações pessoais de mais de 220 milhões de brasileiros foi abertamente colocado à venda em um fórum na internet. Conforme a descrição no site, as informações comercializadas teriam sido roubadas da Serasa Experian. Tal evento resultou no maior caso de vazamento de dados da história do Brasil.

Ao passo em que a Serasa se limita a negar qualquer relação com o incidente, o que se percebeu foi a inércia do poder público, que nada fez para coibir ou mitigar esses incidentes, em especial, a Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

O presente estudo descortina algumas constatações empíricas desse particular cenário de profunda incerteza e insegurança quanto à integridade de dados pessoais, após o advento da Lei Geral de Proteção de Dados (LGPD).

2. O Megavazamento de 223 milhões cadastros pessoais no Brasil

Em janeiro de 2021, a população brasileira descobriu que um enorme vazamento de dados pessoais expôs o CPF de mais de 220 milhões de brasileiros. Tal fato foi amplamente noticiado por inúmeras reportagens e publicações, constatando que a empresa "Serasa Experian S/A" permitiu que houvesse o acesso indevido a dados pessoais dos seus milhões de usuários para além das finalidades em que se propôs. Desse modo a possibilitar que terceiros obtivesse de graça informações pessoais de seu banco

de dados, tais como o endereço residencial dos usuários, dados de compra, CPF, cartão de crédito, dentre outras (VENTURA, 2021).

Conforme pode ser observado na referida reportagem, a própria Serasa Experian S/A admite a existência e extensão do problema ao reconhecer que tinha conhecimento que o arquivo complicado em 2019 possuía dados de 223,74 milhões de CPFs distintos. Tem-se, portanto, uma extensão incalculável dos danos, haja vista que população afetada é maior do que a própria população brasileira em si, uma vez que base de dados também inclui falecidos. Não suficiente, os dados vazados estão disponíveis na internet aberta, e não na dark web, tendo sido o link de acesso indexado até pela busca do Google. Todos esses fatos de amplo conhecimento da empresa.

No entanto, apesar de toda uma gama de indícios que apontam para a base de dados mantida pela empresa, a Serasa não admitiu que a falha tenha sido por ela ocasionada[124], tampouco entrou em contato com os seus clientes e usuários sobre como foram acessados os seus dados, quais dados foram levados, quais os mecanismos de segurança aplicados e quais as medidas de mitigação de riscos foram aplicadas, insistindo de que não há falha de segurança advinda de sua base de dados[125].

Em virtude desse incidente, praticamente todos os dados dos cidadãos brasileiros, vivos e mortos, foram expostos, abrindo a possibilidade para a ocorrência de inúmeras fraudes praticadas por terceiros mal-intencionados que detenham essas informações. Não obstante, conforme noticiado, ainda foi possível verificar outra vulnerabilidade em decorrência do incidente, a qual permitiria a terceiros o acesso a informações detalhadas sobre cartões utilizados pelos usuários como forma de pagamento, bem como prints de salários, entre outros dados que causem exposição danosa.

Insta ressaltar que diversas autoridades nacionais também foram vítimas do incidente, dentre as quais pode-se destacar: os ministros do Supremo Tribunal Federal, os chefes dos demais poderes, e até o Presidente da República. Assim, tem-se que não apenas os dados cadastrais, mas todas as informações econômicas, previdenciárias, fiscais, os perfis em redes sociais, o escore de crédito e a fotografia pessoal de cada um dos 11 ministros do Supremo Tribunal Federal foram colocados à venda na internet, em decorrência do megavazamento (CONSULTOR JURÍDICO, 2021).

Conforme a análise realizada pela empresa de segurança Syhunt, os arquivos disponibilizados pelo hacker envolvido no vazamento configuram uma espécie de "catálogo" das informações obtidas no incidente, de modo que não é possível verificar a identidade ou o número de pessoas envolvidas no vazamento, somente sendo possível auferir a legitimidade das informações ao se efetivar a compra.

---

[124] "Em comunicado ao Tecnoblog, a Serasa Experian diz: 'estamos cientes de alegações de terceiros sobre dados disponibilizados na dark web; conduzimos uma investigação e neste momento não vemos nada que indique que a Serasa seja a fonte" (VENTURA, 2021).

[125] Nota do Serasa acerca do vazamento presente em reportagem da CNN Brasil: "Fizemos uma investigação aprofundada que indica que não há correspondência entre os campos das pastas disponíveis na web com os campos de nossos sistemas onde o Score Serasa é carregado, nem com o Mosaic. Além disso, os dados que vimos incluem elementos que nem mesmo temos em nossos sistemas e os dados que alegam ser atribuídos à Serasa não correspondem aos dados em nossos arquivos". (VENTURA, 2021).

Ainda segundo a Syhunt, foram um total de 223 milhões de brasileiros expostos, de modo que as informações estão divididas em 37 categorias, que compõem um Banco de Dados de aproximadamente 650GB, e cerca de 3KB de dados por pessoa. Além de um total de 159 milhões de brasileiros com detalhes de telefone expostos. Dentre os dados pessoais expostos, tem-se informações conforme as seguintes categorias: nome da pessoa, CPF, sexo, data de nascimento, nome do pai, nome da mãe, estado civil (básico); e-mail; telefone; endereço; "Mosaic"; emprego; score de crédito; registro geral; título de eleitor, escolaridade; empresarial; Receita Federal; classe social; estado civil; emprego; afinidade; modelo analítico; poder aquisitivo; fotos de rostos; servidores públicos; cheques sem fundos; devedores; Bolsa Família; universitários; conselhos; domicílios; vínculos; LinkedIn; salário; renda; óbitos; IRPF; INSS; FGTS; CNS; NIS e PIS/PASEP (DARAGON; SYHUNT, 2021).

Assim, não restando dúvidas que este configura como o maior, mais sério e relevante vazamento de dados pessoais da história da história do Brasil, ensejando uma resposta real ao incidente, tal como medidas de mitigação dos impactos que o megavazamento tem na vida de praticamente toda a população brasileira, além de um alerta em escala mundial quanto à necessidade de uma cultura de privacidade (SERASA EXPERIAN, 2021).

3. Proteção ao crédito e monitoramento de dados pessoais: gestão de riscos cibernéticos como prática de mercado

Segundo dados da Associação Brasileira de Internet (ABRANET), apenas entre os meses de janeiro a setembro de 2020, o Brasil teve mais de 3,4 bilhões de tentativas de ataques cibernéticos, (ABRANET, 2020). A própria Serasa Experian tem ciência que o número de ameaças cibernéticas aumentou 394% em 2020 em relação a 2019, com base no levantamento da empresa Apura Cybersecurity (SERASA EXPERIAN, 2021).

Em que pese a Serasa já estivesse envolvida em incidentes de segurança da informação em 2021, inclusive no megavazamento de dados considerado o maior da história do país, de acordo com material produzido pela Serasa Experian, com o intuito de promover a venda de seus Cerificados Digitais, o vazamento de dados coloca em risco as informações pessoais dos usuários, configurando uma grave violação. Nesse sentido, o relatório elaborado pela Apura contabilizou mais de 958 mil CPFs, 592 mil cartões internacionais, 262 mil cartões nacionais e 220 milhões de credenciais de acesso de usuários, que foram coletados pelo BTTng[126] (SERASA EXPERIAN, 2021).

Assim, é possível observar uma prática de mercado um tanto contraditória e até abusiva, considerando que além de divulgar a importância na aquisição de sua linha de certificados digitais para fins de segurança da informação e prevenção a dados pessoais, também comercializa soluções para que o consumidor monitore caso exista

[126] BTTng, ou Boitatá Next Generation, é uma plataforma de Open Source Intelligence, desenvolvida e mantida pela Apura Cybersecurity Intelligente, que permite obter informações sobre as mais diversas ameaças cibernéticas, por meio de uma coleta, busca e indexação automatizada das informações existentes na web, redes sociais e até deep/dark web. Mais informações no link: https://apura.com.br/#:~:text=O%20BTT%20NG%20%E2%80%93%20tamb%C3%A9m%20conhecido,sociais%20e%20deep%2Fdark%20web.

incidentes como o caso em foco, por meio de um produto denominado "Serasa Premium".[127]

Portanto, conquanto fortes elementos apontem para a constatação de que a Serasa Experian esteja concorrendo diretamente para a ocorrência de incidentes envolvendo dados pessoais dos consumidores, como já demonstrado, tais indicativos são reforçados constantemente à medida que golpes e novos incidentes (vazamentos) são registrados. Em outros termos, tem-se que quanto mais incidentes ocorrerem, maior será o interesse dos titulares de dados pessoais contratarem serviços que o notificam caso seu CPF foi ou está sendo usado sem seu consentimento, tendo que pagar por cada consulta ou contratar um pacote, como o oferecido pela Serasa.

Para além, há de se ressaltar que a Experian, empresa mãe que detém a Serasa, e atua em 45 países (TADEU, 2021), pode pagar multa monumental no Reino Unido, por práticas similares, de modo que ela tem até julho desse ano para cumprir as determinações da Autoridade de Proteção de Dados do Reino Unido (Ibidem). Isso se dá, pois em outubro de 2020, o órgão supervisor de proteção de dados no país (ICO) alertou a Experian para cumprir um aviso de execução ou enfrentar a multa, que pode chegar a 4% do faturamento total anual mundial, com base no Regulamento Geral de Proteção de Dados da União Europeia (GDPR) por usar ilegalmente dados de clientes.

Segundo informações encontradas no relatório oficial do órgão de supervisão do Reino Unido, o Information Commissioner's Office (ICO), a execução decorre de uma investigação de dois anos sobre as atividades das três grandes agências de referência de crédito (CRAs): Experian, TransUnion e Equifax. As três empresas foram encontradas "negociando, enriquecendo e aprimorando" dados dos consumidores sem consentimento expresso, vendendo-os em produtos projetados para empresas, partidos políticos e instituições de caridade para atingir indivíduos específicos e construir perfis sobre eles.[128]

Além dessas práticas que já estão sendo combatidas em nível mundial, a Serasa Experian foi notificada pelo PROCON de São Paulo por estar promovendo uma campanha em seu portal de Internet na qual a empresa solicita a senha do internet banking para que os usuários participem de um "estudo" disponibilizado no mesmo

---

[127] Conforme descrição constante do mesmo site: "ao monitorar o CPF, o Serasa Premium informa sobre movimentações e negativações encontradas em seu nome. Você recebe um alerta via SMS e e-mail sempre que seu CPF: For retirado do cadastro de inadimplência; Seja vinculado a um protesto em cartório, ação judicial ou cheque sem fundo. Caso você não reconheça qualquer uma dessas movimentações, pode ser um sinal de fraude. E você ganha tempo para se proteger das ações dos criminosos". Disponível em: <https://www.serasa.com.br/premium/monitoramento-cpf>. Acesso em: 10 mar. 2021.

[128] Segundo o relatório as empresas também estavam usando as informações coletadas para referência de crédito em seu próprio marketing direto, e gerando novas informações via perfil. Esse processamento de dados "invisível" afetou milhões de adultos britânicos: não só não foram informados sobre como seus dados estavam sendo usados, mas os CRAs também interpretaram mal a lei para aplicar bases legais incorretamente para processar os dados das pessoas. Tanto a Equifax quanto a TransUnion fizeram melhorias em suas práticas de dados enquanto retiravam alguns produtos, no entanto, a Experian recusou, e é por isso que agora está enfrentando o aviso de execução. Até julho de 2021, a empresa precisa apenas informar aos clientes que detém seus dados e como pretende usá-los para fins de marketing. Até janeiro de 2021, também deve parar de usar dados derivados de suas verificações de crédito para marketing direto, de acordo com o regulador. Outras condições do aviso incluem: interromper o processamento de dados coletados ilegalmente, excluir quaisquer dados coletados com consentimento, mas que agora está sendo usado sob uma base legal de "interesses legítimos" e esclarecer aos clientes quais dados ele possui, de onde ele veio e para que está sendo usado (ICO, 2021).

portal onde é possível conferir dados referentes ao CPF do cidadão. Segundo o portal G1, o PROCON "quis saber a finalidade da campanha, público-alvo, as informações que foram colocadas e qual foi o tratamento desses dados, levando em conta a vigência da Lei Geral de Proteção de Dados" (ROHR, 2021).

Em resposta a empresa apontou que, de fato, pede a senha do internet banking para que os usuários participem de um "estudo", mas afirma "que não é passível de ocorrer fraudes mediante a utilização da senha compartilhada para a realização desse estudo de participação voluntária". (ROHR, 2021). Contudo, a Serasa já havia se envolvido em outras polêmicas similares, como no caso do megavazamento de dados de 2021, na qual o hacker afirmou que obteve milhões de dados de brasileiros com a base de dados da empresa (COUTO, 2021).

Apesar das reiteradas tentativas da Serasa em negar que o vazamento tenha origem de sua base de dados, insta rememorar toda a gama de riscos trazidos pelo episódio conhecido como "Serasa Experian Full Database" em questão, uma vez que cada porção do vazamento traz dados de exatamente 5.593.481 CPFs e 1.004.596 CNPJs. Ao todo, são 960 GB em arquivos (96 GB quando comprimidos)" (VENTURA, 2021).

Ressalte-se que o hacker Marcos Roberto Correia da Silva (sob o pseudônimo "VandaTheGod") foi preso pela Polícia Federal no âmbito da Operação Deepwater, mas até hoje não se esclareceu nada sobre a origem dos dados. Rapidamente, esse escândalo foi sendo esquecido de forma conveniente e praticamente desapareceu da mídia, além de não ter sido consistentemente apurado pelas autoridades administrativas, tais como ANPD, CADE e SENACON-MJ.

De acordo com o Data Breach Investigations Report (Verizon), a maioria dos ciberataques é desencadeada por estranhos, insiders, parceiros da empresa, grupos do crime organizado e grupos afiliados. Com efeito, as ameaças podem estar mais próximas do que se imagina, com o Brasil ocupando atualmente a segunda posição no ranking dos países que mais sofrem ataques cibernéticos, de acordo com o Mapa Kaspersky Lab[129].

4. O silêncio da Autoridade Nacional de Proteção de Dados

Diante desse cenário, observa-se que o silêncio da Autoridade Nacional de Proteção de Dados (ANPD) é o mais eloquente: apesar do Brasil ocupar a 6ª colocação no ranking dos países mais afetados por vazamentos de dados em 2021, de acordo com a Surfshark (CAMURÇA, 2022), não houve sequer uma única punição aplicada a qualquer empresa ou órgão público desde sua criação e efetiva atuação, tanto no cenário nacional quanto em termos globais.

Há de se constar que os bancos de dados das empresas de proteção de crédito foram criados justamente para realizar o tratamento de proteção de dados pessoais e de empresas. Não à toa sempre houve o seu enquadramento com o Código do Consumidor, de 1990, e com a Lei do Cadastro Positivo, de 2011. Com tudo, a existência de uma Lei específica de proteção de dados traz consigo a esperança de mais segurança aos usuários, tendo em vista, inclusive, o princípio da segurança, uma vez que este deveria impulsionar o setor de proteção ao crédito a desenvolver esforços

[129] Informação do dia 05 de abril de 2022, o mapa pode ser acessado no link: https://cybermap.kaspersky.com/

para mitigar os riscos de segurança ou vazamentos de informações, sobretudo diante do crescimento de ataques cibernéticos.

Para tanto, é necessário que haja uma atuação efetiva da autoridade de proteção de dados, a fim de fiscalizar as empresas, razão pela qual o funcionamento da ANPD se faz essencial. Sem a condução estratégica e educativa da ANPD, as múltiplas interpretações de outras esfereas públicas tenderão a causar insegurança jurídica e milhares de ações judiciais, que poderiam ser dirimidas em boa parte dos casos por instruções e orientações prévias da autoridade competente (SFIER, 2020).

Em pesquisa realizada pelo Data Privacy Benchmark Study, de 2020, restou comprovado que há inúmeros benefícios obtidos pelas empresas que já adotam práticas para a redução de riscos relacionados à segurança dos dados, tais como recebimento de 2,7 vezes o investimento inicial em proteção de dados (CISCO, 2020).

Ao tempo em que o volume de crimes cibernéticos escala assustadoramente, como é de geral conhecimento, boa parte deles são perpetrados com a utilização de dados pessoais que constam nessas bases envolvidas no caso concreto. Daí a importância da produção de prova técnica robusta, algo que deveria ter sido já estabelecido ou minimamente justificado pelas autoridades oficiais (G1, 2022).

Nesse sentido, como explicitou o professor Rafael Zanatta (Diretor da Data Privacy Brasil), a prioridade deveria ser, desde o primeiro momento, "investigar a origem para avaliar as formas de responsabilização de quem está por trás do vazamento, partindo dos indícios já existentes". Ainda segundo o especialista, seria necessário "delimitar, por meio de auditoria da ANPD, os servidores da Serasa e as bases [vazadas] para responder qual o grau de similitude" (VALENTE, 2021).

Destaque-se que a opinião acima foi apresentada em 2021, quando ocorreu o incidente. Àquela altura, a Ordem dos Advogados do Brasil (OAB) encaminhou ofício à ANPD, solicitando providência para apurar o caso. Contudo, atualmente, em pleno 2022, ainda é possível encontrar os dados de centenas de milhões de brasileiros que foram vazados naquela ocasião, e continuam sendo vendidos na web aberta e na deep web, o que é muito grave (KNOTH, 2022).

Como advertiu o advogado Omar Kaminski, um dos mais respeitados especialistas sobre o tema no Brasil, ao referir o evento como catastrófico: "Não se pode mais tolerar esse tipo de ocorrência como se fosse normal ou aceitável. Não é, nem pode ser. Se a desculpa era a ausência de uma lei específica, habemus legem" (SANTOS, 2021).

5. Caso Equifax: convergências com o monumental incidente brasileiro

Diante desse contexto, perfeitamente possível é a comparação do vazamento ocorrido no Brasil ao que aconteceu nos Estados Unidos em 2017, quando os dados da empresa de gestão de crédito Equifax, portanto, com atuação análoga à SERASA, foram vazados e comprometeram a privacidade de 147 milhões de consumidores, entre EUA, Canadá e Reino Unido.

Sendo uma das três maiores agências de gestão de créditos dos EUA, o vazamento de dados que resultou também na exposição de números de cartão de

crédito de aproximadamente 209 mil consumidores é considerado como sem precedentes, tanto em escopo quanto em seriedade, gerando uma onda de problemas em escala nunca vista anteriormente nos EUA (ELETRONIC PRIVACY INFORMATION CENTER, 2020).

Em 28 de janeiro de 2019, a Corte do Distrito Norte da Geórgia (EUA) emitiu uma decisão na Ação Coletiva da Equifax (Consolidated Consumer Class Action), permitindo que as reivindicações das vítimas da Equifax fossem atendidas (GESSER, ROBLES, 2021). O Tribunal rejeitou os argumentos da empresa de que os danos experimentados pelos titulares de dados deveriam ser atribuídos aos hackers e poderiam ter sido causados por violações de dados em outras empresas.

No entanto, a Corte Distrital observou que permitir que as empresas "confiem em outras violações de dados para derrotar uma conexão causal" criaria um incentivo perverso para as empresas: desde que ocorram violações de dados suficientes, empresas individuais nunca seriam consideradas responsáveis.

O Tribunal concluiu que, devido ao risco previsível de violação de dados, a Equifax devia aos consumidores o dever legal independente de tomar medidas razoáveis para proteger suas informações pessoais sob a custódia da Equifax. Ao fazê-lo, o Tribunal concluiu que a doutrina da necessária perda econômica não era um obstáculo à reparação dos consumidores porque a Equifax tinha um dever independente de salvaguardar informações pessoais.

Desse modo, ao concluir esse dever da Equifax de cuidado que existe no contexto de violações de dados, a Corte tornou as reivindicações de negligência uma opção mais viável para os reclamantes de violação de dados. Essa mudança de interpretação culminou com o histórico acordo celebrado com a Federal Trade Comission dos EUA e outros estados (EXAME, 2021).

Assim, em 2019, a empresa celebrou um acordo com a Comissão Federal de Comércio (FTC), autoridade de defesa dos consumidores, e com os Estados, para o pagamento de cerca de 700 milhões de dólares (R$ 3,7 bilhões) e a responsabilidade da própria empresa montar uma central de atendimento para os lesados, pelo período de 4 (quatro) anos. Contudo, apesar do acordo com o FTC ter, em tese, solucionado e encerrado a situação, ocorre que, na prática, os consumidores serão os menos beneficiados, uma vez que a maioria dos indivíduos tem a chance mínima de obter alguma recompensa e/ou reparação dos danos (LEYDEN, 2022), praticamente irreversíveis, ocasionados em virtude do vazamento dos dados da Equifax.

Ainda que o resultado não tenha sido o mais satisfatório para os consumidores, não restam dúvidas que o caso da Equifax cria um paradigma, e seus reflexos, quaisquer sejam, merecem atenção. Assim como ocorreu com o Caso Equifax, é possível reconhecer que a responsabilidade da Serasa decorre do fato da empresa ter se omitido de tomar todas as medidas razoáveis necessárias para prevenir atividades que pudessem resultar na violação da legislação que ora se evidencia.

No caso brasileiro, observa-se o direcionamento na contramão do vazamento americano, uma vez que não há uma única empresa enfrentando investigação e

responsabilização e, no caso da Serasa Experian, um agravante: ela continua com oferta de produtos de monitoramento de fraudes envolvendo dados pessoais. Verifica-se, portanto, que os negócios dos bureaus de cédito se perpetuam, tal como a sua reiterada inobservância do presumível dever de cuidado com os seus clientes e usuários, titulares de dados. De tal modo que, em todos os seus âmbitos, seguem ferindo a inviolabilidade de dados, a privacidade, a intimidade, a vida privada deles, colocando em risco a sociedade brasileira.

6. Sem conclusão? Os próximos desafios e a proteção de dados pessoais

Assim, ao invés de conceber relações recíprocas e construtivas entre a empresa e o consumidor, os produtos e serviços do capitalismo de vigilância passaram a estabelecer "ganchos", nos quais os usuários são atraídos, para as operações extrativistas de dados, nas quais as experiências pessoais de cada um são condicionadas como meios para fins de outros. Assim, os usuários deixam de exercer o papel de cliente, passando a ser o objeto de extração da matéria prima que proporciona o superávit necessário para o capitalismo de vigilância (ZUBOFF, 2021, p. 22).

Nesse sentido, importa salientar que o capitalismo de vigilância, forma de mercado da economia digital, de modo a se observar a estruturação de um novo tipo de comércio que conta com a interferência na espera da personalidade por meios de modificação comportamental, a partir do qual refaz a natureza humana em nome da certeza do lucro (ZUBOFF, 2021, p. 364).

Em retomada ao maior incidente do gênero em "solo" nacional, é possível concluir que deixar empresas investigadas impunes seria o mesmo que conceder status de permissivo legal para as más práticas verificadas em suas rotinas, inclusive diversas modalidades de ilícitos. É preciso ter em mente o que está em jogo: valores fundamentais do constitucionalismo tais como a privacidade, a liberdade de expressão, a isonomia e princípio democrático, apenas para ficar em alguns.

Para além, o próprio direito à proteção de dados pessoais, que atualmente ostenta status constitucional, por força da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, sob a égide do princípio do direito à autodeterminação informativa, na trilha do clássico conceito erigido pela Corte Constitucional, na Sentença da Lei do Censo (BVerfGE 65, 1, "Volkszählung")[130] (RUARO; RODRIGUEZ, 2011), implica na necessária imposição de sanções cíveis, com base na legislação em pleno vigor no Brasil, consolidando a nítida evolução em relação ao atual estágio civilizatório da sociedade algorítmica.

Em paralelo, importa salientar que sendo o direito à proteção de dados pessoais, uma dimensão à parte ao direito à privacidade, este ecoa enquanto dimensão do direito à personalidade, de tal modo que a impunidade à nítida negligência a proteção dos dados pessoais, implica na redução do valor do próprio indivíduo em si. Assim, ainda que as alegações da Serasa fossem verdadeiras, isto é, que os dados não teriam saído de servidores ou de quaisquer estabelecimentos dela, em razão do sistema protetivo de dados que cercam todos os tratamentos pela referida empresa, dessume-se sua

[130] Para uma análise detalhada do caso, cf. MARTINS, Leonardo. (org.) **Cinquenta anos de Jurisprudência do Tribunal Constitucional federal Alemão**. Montevidéu: Fundação Konrad Adenauer, 2005, p. 244.

responsabilidade com base na tese da responsabilidade solidária em razão de sua atividade econômica.

Afinal, cabe questionar: que procedimentos foram adotados pela empresa para apresentar tal conclusão de que "não teria sido a origem do vazamento"? E se tivesse sido confirmada como tal, quais seriam as medidas de contenção e mitigação dos danos? Não resta claro qual seria ou deveria ser a resposta ao incidente, o que descortina a fragilidade da governança da multinacional, de que seu accountability é praticamente inexistente e, sobretudo, que seu compliance é deficitário.

A política específica de conformidade à Lei Geral de Proteção de Dados é evidentemente uma preocupação secundária de muitas corporações, que sequer indicam o denominado Encarregado de Proteção de Dados, em flagrante violação à Lei 13.709/2018. Com efeito, os direitos dos titulares são de caráter personalíssimo, e estão diretamente conectados com a dignidade humana de cada um deles. Assim, quaisquer vazamentos ou tratamentos ilegais os atingem, de forma única, indisponível e inalienável e, coletivamente, desfere um golpe à sociedade que se vê desprotegida pelos agentes de tratamento.

Portanto, o que se observa é que, seja qual for o cenário, empresas responsáveis pelo armazenamento de grande volume de dados precisam responder objetivamente pelas informações eventualmente coletadas. Afinal, direta ou indiretamente, concorrem para a ilegalidade e não se tem notado aqui boas práticas no desenvolvimento dos seus serviços, demonstrando descaso com o episódio, quando deveria realizar todos os esforços necessários para mitigar os deletérios efeitos do vazamento, em consonância como o primado do razoável dever de cuidado.

Referências

ABRANET, Redação da. Brasil teve mais de 3,4 bilhões de tentativas de ataques cibernéticos em 2020. Associação Brasileira de Internet, 2020. Disponível em: https://www.abranet.org.br/Noticias/Brasil-teve-mais-de-3%2C4-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2020-3152.html?UserActiveTemplate=site#.YkyUnsjMJpg Acesso em: 05 abr. 2022.

BELLI, Luca. The largest personal data leakage in Brazilian history: why the rest of the world should be worried, and think hard about how to create a data protection culture. Open Democracy, 2021. Disponível em: https://www.opendemocracy.net/en/largest-personal-data-leakage-brazilian-history/ Acesso em: 05 abr. 2022.

CAMURÇA, Francisco. Brasil se mantém no top 10 mundial de países afetados por vazamentos de dados. We Live Security, 2022. Disponível em: https://www.welivesecurity.com/br/2022/01/19/brasil-se-mantem-no-top-10-mundial-de-paises-afetados-por-vazamentos-de-dados Acesso em: 10 fev. 2022.

CONSULTOR JURÍDICO. Vazamento do fim do mundo: após megavazamento, dados de ministros do Supremo são postos à venda. Consultor Jurídico, 2021. Disponível em: https://www.conjur.com.br/2021-fev-02/megavazamento-dados-ministros-stf-sao-postos-venda Acesso em: 8 fev. 2021.

COUTO, Marcus. Serasa pede senhas bancárias para 'estudo'; Procon questiona. Yahoo finanças, 2021. Disponível em: https://br.financas.yahoo.com/noticias/serasa-pede-senhas-bancarias-para-estudo-procon-questiona-141116829.html Acesso em: 10 mar. 2021.

DARAGON, Felipe; SYHUNT, Equipe. O megavazamento do Brasil. Syhunt, 2021. Disponível em: https://www.syhunt.com/pt/index.php?n=Articles.BrazilDataLeak2021 Acesso em: 05 abr. de 2022.

ELETRONIC PRIVACY INFORMATION CENTER. Epic, 2020. Equifax Data Breach. Disponível em: < https://archive.epic.org/privacy/data-breach/equifax/ Acesso em: 05 abr. 2022.

Data Privacy Benchmark 2020 da Cisco confirma vantagens financeiras positivas a partir de práticas corporativas. Cisco, 2020. Disponível em: https://news-blogs.cisco.com/americas/pt/2020/01/30/estudo-data-privacy-benchmark-2020-da-cisco-confirma-vantagens-financeiras-positivas-a-partir-de-praticas-corporativas-em-privacidade-de-dados/#:~:text=%E2%80%93%2030%20de%20janeiro%20de%202020,adotam%20pr%C3%A1ticas%20fortes%20de%20privacidade Acesso em: 05 abr. 2022.

EXAME ONLINE, 22 jul. 2021. Disponível em: https://exame.com/negocios/equifax-pagara-ate-us-700-milhoes-por-vazamento-de-dados-pessoais/ Acesso em: 10 fev. 2022.

G1. Brasileiros sofrem uma tentativa de fraude a cada 7 segundos; saiba como se proteger. G1, 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/01/26/brasileiros-sofrem-uma-tentativa-de-fraude-a-cada-7-segundo-saiba-como-se-proteger.ghtml
Acesso em: 10 fev. 2022.

GESSER, Avi; e ROBLES, David. The Rise of Cyber Negligence Claims: Plaintiffs Find Receptive Judges by Going Back to Basics. NYU Law's Program on Corporate Compliance and Enforcement. Disponível em: https://wp.nyu.edu/compliance_enforcement/2019/03/06/the-rise-of-cyber-negligence-claims-plaintiffs-find-receptive-judges-by-going-back-to-basics/
Acesso em: 8 fev. 2021.

HARARI, Yuval Noah. Homo Deus: uma breve história do amanhã. Trad. Paulo Geiger. Rio de Janeiro: Companhia das Letras, 2016.

ICO takes enforcement action against Experian after data broking investigation. Ico, 2020. Disponível em: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation/ Acesso em: 10 mar. 2021.

KNOTH, Pedro. Megavazamento de CPFs: um ano depois, ainda há perguntas sem resposta. Tecnoblog, 2022. Disponível em: https://tecnoblog.net/especiais/pedro-knoth/megavazamento-de-223-milhoes-de-cpfs-um-ano-se-passou-e-ainda-ha-perguntas-sem-resposta/ Acesso em: 10 fev. 2022.

LEYDEN, John. Equifax data breach: consumers unlikely to benefit financially from final settlement. The Daily Swig, 2022. Disponível em: https://portswigger.net/daily-swig/equifax-data-breach-consumers-unlikely-to-benefit-financially-from-final-settlement Acesso em: 05 abr. 2022.

ROHR, Altieres. Procon-SP notifica Serasa por estudo que solicitou senha bancária; empresa nega risco a usuários. G1, 2021. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/03/04/procon-sp-notifica-serasa-por-estudo-que-solicitou-senha-bancaria-empresa-nega-risco-a-usuarios.ghtml Acesso em: 10 mar. 2021.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. Nada a esconder? O direito à proteção de dados frente a medidas de segurança pública e intervenção estatal. Portal de e-governo, inclusão digital e sociedade do conhecimento, 2011. Disponível em: http://www.egov.ufsc.br/portal/conteudo/nada-esconder-o-direito-à-proteção-de-dados-frente-medidas-de-segurança-pública-e-intervenç

SANTOS, Rafa. Vazamento de dados é grave e seu impacto será sentido por anos, dizem especialistas. Consultor Jurídico, 2021. Disponível em: https://www.conjur.com.br/2021-fev-01/vazamento-dados-grave-impacto-sentido-anos Acesso em: 8 fev. 2021.

SERASA EXPERIAN. Cibergolpes cresceram 400% em 2020 e devem aumentar em 2021, mostra estudo de empresa especializada. Serasa Experian, 2021. Disponível em: https://serasa.certificadodigital.com.br/blog/mercado/cibergolpes-cresceram-400-em-2020-e-devem-aumentar-em-2021-mostra-estudo-de-empresa-especializada/ Acesso em: 04 abr. 2022.

SFIER, Elias. O compromisso das empresas de serviços de proteção ao crédito com a LGPD. JOTA, 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-compromisso-das-empresas-de-servicos-de-protecao-ao-credito-com-a-lgpd-04112020#:~:text=Na%20implementa%C3%A7%C3%A3o%20da%20LGPD%2C%20o,jur%C3%ADdica%20na%20adequa%C3%A7%C3%A3o%20%C3%A0%20lei Acesso em: 04 abr. 2022.

TADEU, Erivelto. Experian pode pagar multa de US$ 26 mi por suposta infração à GDPR. Ciso Advisor, 2020. Disponível em: https://www.cisoadvisor.com.br/experian-pode-pagar-multa-de-ate-us-26-mi-por-suposta-infracao-a-gdpr/ Acesso em: 05 abr. 2022.

VALENTE, Jonas. OAB pede investigação do vazamento de dados de 220 milhões de pessoas. Valor Investe, 2021. Disponível em: < https://valorinveste.globo.com/mercados/brasil-e-politica/noticia/2021/01/29/oab-pede-investigacao-do-vazamento-de-dados-de-220-milhoes-de-pessoas.ghtml> Acesso em: 10 fev. 2022.

VENTURA, Felipe. Exclusivo: vazamento de 223 milhões de CPFs é vendido em "promoção" por US$ 30 mil. Terra, 2021. Disponível em https://www.terra.com.br/noticias/tecnologia/exclusivo-vazamento-de-223-milhoes-de-cpfs-e-vendido-em-promocao-por-us-30-mil,268e60812a87e0826d8a43fb956cf8ddtr08oz1c.html Acesso em: 05 abr. de 2022.

ZUBOFF, Shosana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira de poder. 1ª Ed. Rio de Janeiro: Intrínseca, 2021.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, Cambridge, n. 30, pp. 75-89, 2015.

Consideraciones breves sobre los fundamentos de la propuesta de Ley de Inteligencia Artificial de la Comisión Europea[131]

Manuel David Masseno[132]

RESUMO

Este estudo destinou-se a colocar à disposição dos parlamentares mexicanos, assim como dos demais parlamentares ibero-americanos, uma síntese informativa, crítica e contextualizada do procedimento legislativo em curso na EU – União Europeia relativamente à regulação da IA – Inteligência Artificial, também com utilidade para os pesquisadores. Para tal, foi seguindo fundamentalmente o método histórico-jurídico, mas com aberturas aos métodos comparativo e hermenêutico. Em suma, explica como é viável passar de uma perspectiva assente em princípios para uma assente em regras, inclusivamente em um campo tão novo e desafiantes como a IA, expondo as vantagens, e as fraquezas, de uma abordagem de cima para baixo no que respeita a uma tecnologia de alto risco para a própria Humanidade.

PALAVRAS-CHAVE

Inteligência artificial; União Europeia; Dignidade humana; Processo Legislativo; Riscos

---

[131] Este texto corresponde à intervenção realizada no *Foro Internacional "Las Repercusiones de la Ciencia y la Tecnología para la Innovación en el Derecho"*, para a Câmara dos Deputados do México e para Facultade de Direito da UNAM – Universidade Nacional Autônoma do México, no día 6 de abril de 2022, estando também em publicação nas respetivas Atas. Por essa razão, não se trata de um trabalho de natureza propriamente acadêmica, mas sim de uma síntese, à qual foram acrescentadas as fontes documentais. Para um desenvolvimento crítico de estas questões, em espanhol, sobretudo no que se refere à *Proposta de Regulamento Inteligência Artificial*, sugiro a leitura dos seguintes artigos: De Miguel Asensio, P. Propuesta de Reglamento sobre Inteligencia Artificial. *La Ley - Unión Europea*, 2021, 92, Cotino Hueso, L. Un análisis crítico constructivo de la Propuesta de Reglamento de la Unión Europea por el que se establecen normas armonizadas sobre la Inteligencia Artificial (*Artificial Intelligence Act*). *Diario La Ley*, 26/06/2021; além de García García, S. Una aproximación a la futura regulación de la inteligencia artificial en la Unión Europea. *Revista de Estudios Europeos*, 2022, 79, pp. 304-323.

[132] Professor Adjunto e Encarregado da Proteção de Dados do Instituto Politécnico de Beja, em Portugal. <https://orcid.org/0000-0001-8861-0337> / <masseno@ipbeja.pt>.

Brief Considerations on the Foundations of the proposal of Artificial Intelligence from the European Commission

Manuel David Masseno

ABSTRACT

This study intents to make available to Mexican legislators, as well as other Ibero-American legislators, an informative, critical, and contextualized synthesis to the legislative procedure underway at the EU - European Union regarding the regulation of AI - Artificial Intelligence, being also useful for researchers on these subjects. Thus, the historical research method was the mainly followed, but the comparative and hermeneutic methods had a role too. In short, it shows how is viable to go beyond a principles-based approach into a rules-based approach, even in a field as new and challenging field as AI, exposing the advantages, and shortcomings, of a top-down procedure concerning the regulation of a technology with the highest-risks even for mankind.

KEYWORDS

Artificial Intelligence; European Union; Human Dignity; Legislative Procedure; Risks

1. La "dignidad humana" como piedra angular de la Propuesta

En relación con nuestro objeto, el ordenamiento de los sistemas (algoritmos) de IA (Inteligencia Artificial) según criterios éticos, nos ocuparemos sumariamente de la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión Europea (COM(2021) 206 final, de 21de abril)[133], de la Comisión Europea.

Explícitamente, la Propuesta[134] está fundada en la prevención y control de los riesgos para los Derechos Fundamentales, como expresión del valor nuclear de la Unión Europea, la "dignidad humana" (Art. 2 del Tratado de la Unión Europea (TUE) y Art. 1 de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE)).

Cumple también subrayar que la iniciativa tuvo en especial consideración y resulta coherente con los últimos planteamientos del Parlamento Europeo en la Resolución sobre el Marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL), de 20 de octubre) y también del Consejo en las Conclusiones de la Presidencia [alemana] La Carta de los Derechos Fundamentales en el contexto de la inteligencia artificial y el cambio digital (11481/20, de 21 de octubre), la cual pone en evidencia en consenso alcanzado en el seno de los Gobiernos de los Estados-Miembros.

Además, se asumió que, de esta opción, de naturaleza constitucional, puedan resultar desventajas potenciales para la competitividad global de las empresas europeas respecto a las de Estados Unidos o de China, como ya ocurriera con la protección de datos personales, al adoptarse em Reglamento General sobre Protección de Datos, en 2016[135]. Sin embargo y teniendo en cuenta la experiencia desde 2018 en esa materia, resulta real la posibilidad de las nuevas reglas europeas pasen también a ser "el" punto de referencia / benchmark a nivel global, o por lo menos en los Estados de Derecho.

Asimismo, en la Exposición de motivos y en los Considerandos de la Propuesta, se explicitan parámetros de protección de las personas, con una especial consideración de los más vulnerables, como ocurre con la "protección de los consumidores", de las "personas discapacitadas", de los trabajadores, de los niños y personas mayores o de los refugiados (Arts. 8, 38, 26, 15 y 28 a 31, 24, 25 y 18 y 19, todos de la CDFUE), pero también de las libertades "de pensamiento, de conciencia y de religión", "de expresión

---

[133] Al mismo tiempo, la Comisión Europea presentó la Comunicación [al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones] *Fomentar un planteamiento europeo en materia de inteligencia artificial* (COM(2021) 205 final), con anexos, incluyendo la nueva versión del *Plan coordinado sobre la inteligencia artificial*, de 2018; además de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a las máquinas y sus partes y accesorios (COM(2021) 202 final), también con anexos, la cual tiene en consideración los nuevos riegos que conllevan tecnologías como la IA, Internet de las Cosas (*IoT*) o la robótica.

[134] Según el artículo 289 del *Tratado de Funcionamiento de la Unión Europea* (*TFUE*), "El procedimiento legislativo ordinario consiste en la adopción conjunta por el Parlamento Europeo y el Consejo, a propuesta de la Comisión, de un reglamento, una directiva o una decisión. Este procedimiento se define en el artículo 294"; por otras palabras, en la Unión Europea el órgano ejecutivo tiene la exclusividad del poder de iniciativa legislativa, correspondiendo la decisión final a los representantes de los Pueblos y a los Gobiernos de los Estados-Miembros, en paridad.

[135] El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (*Reglamento general de protección de datos*), el *RGPD*.

y de información", "de las artes y de las ciencias", "a la educación" o, incluso, "de empresa", sin olvidar los correspondientes al "respeto de la vida privada y familiar" o de "protección de datos de carácter personal" (Arts. 10, 11, 13, 14, 16, 7 o 8, también de la CDFUE).

Concretando, tenemos que la Propuesta asienta en criterios de riesgo para los derechos de las personas, con una separación neta entre los sistemas de IA:

__ Prohibidos (los que puedan manipular, incluso subliminarmente, a las personas, sobre todo las más vulnerables, permitan la "puntuación social" o la videovigilancia biométrica en tiempo real e indiscriminada, en el segundo apartado con algunas excepciones, Art. 5);

__ de Alto riesgo (como la "identificación biométrica y categorización de personas físicas", "educación y formación profesional", el "empleo, gestión de los trabajadores y acceso al autoempleo", el "acceso y disfrute de servicios públicos y privados esenciales y sus beneficios" [incluyendo la "solvencia" y "calificación crediticia"], los "asuntos relacionados con la aplicación de la ley", la "gestión de la migración, el asilo y el control fronterizo" y la "administración de justicia y procesos democráticos", Art. 6 y Anexo III), sujetos a reglas estrictas de certificación previa y registro de la actividad, siempre bajo supervisión humana (Art. 8 a 51), las cuales señalaremos a continuación;

__ de Riesgo limitado (como ocurre con los robots conversacionales / chatbots o, los sistemas de identificación biométrica o de emociones, además de los sistemas creadores de ultrafalsos / deepfakes), con la imposición de requisitos de transparencia (Art. 52); y

__ de Riesgo mínimo o nulo (como los videojuegos o los filtros de SPAM), que se quedan fuera del objeto de la Propuesta de Reglamento (Art. 1)

La Propuesta prevé la institución de una gobernanza a cargo de autoridades nacionales de vigilancia, bajo supervisión de la Comisión Europea, la cual estará asistida por un Comité Europeo de Inteligencia Artificial, e incluso de multas administrativas muy altas, de hasta 30 millones de euros o "el 6 % del volumen de negocio total anual mundial del ejercicio financiero anterior, si esta cuantía fuese superior" (Arts. 62 a 72), o sea, un 50% más que las aplicables en materia de protección de datos.

En especial, la creación y utilización de "sistemas de IA de alto riesgo" supone establecer, implantar, documentar y mantener un "sistema de gestión de riesgos" (Art. 9), en especial siempre que conlleven la utilización de técnicas de entrenamiento de modelos con dados (Art. 10), con documentación técnica detallada y actualizada (Art. 11), la conservación de registros automáticos de eventos (Art. 12), mientras que "se diseñarán y desarrollarán de un modo que garantice que funcionan con un nivel de transparencia suficiente para que los usuarios interpreten y usen correctamente su información de salida" (Art. 13) y "alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera consistente en esos sentidos durante todo su ciclo de vida" (Art. 15), incluso para permitir la "vigilancia humana" constante y efectiva (Art. 14).

Lo que deja claro cómo fue seguido un enfoque descendiente [top-down], acercando el enfoque de la Propuesta al Reglamento sobre la Ciberseguridad, de

2019[136], aparatándose del Reglamento general de protección de datos. Lo que nos enseña como instrumentos basados en la prevención y control de riesgos pueden asumir orientaciones distintas, sobre todo si pueden ser complementarios, como ocurre entre los tres reglamentos.

Sin embargo y como resulta de la Comunicación de la Comisión Brújula Digital 2030: el enfoque de Europa para el Decenio Digital (COM(2021) 118 final, de 9 de marzo), más que en aspectos técnicos, los cimientos están, y siempre estarán, en "el respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías" como Valores comunes y fundamentos de la UE (Art. 2 del TUE). Lo mismo consta del Informe sobre la Inteligencia Artificial en la Era Digital (2020/2266(INI)), de la Comisión Especial sobre Inteligencia Artificial en la Era Digital del Parlamento Europeo, de 23 de marzo último, con algunos matices adicionales137.

2. El camino hacia la Propuesta

En la Unión Europea, el primer abordaje normativo de los sistemas de IA resultó de la Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, estableciendo reglas aplicables a las "Decisiones individuales automatizadas" (Art. 15). Además, quedo previsto el derecho al "conocimiento de la lógica utilizada" en esos tratamientos, la llamada "transparencia algorítmica" (Art. 12 a).

Por añadido, los "Principios relativos a calidad de los datos", imponiendo limitaciones al tratamiento indiscriminado y duradero (Art. 6), permitieron una limitación robusta a la introducción indiscriminada de procesos fundados en macrodatos [big data][138].

En 2016, estas mismas reglas y principios fueron profundizados, con matices, con el Reglamento General de Protección de Datos. Ante todo, en lo que se refiere a las garantías previstas para tratamientos conducentes a "Decisiones individuales automatizadas, incluida la elaboración de perfiles" (Art. 22). A lo que acrecen los "Derechos del interesado" a la "transparencia de la información", en particular "la existencia de decisiones automatizas, incluida la elaboración de perfiles" (Arts. 13 y 14) y el "derecho a oponerse", señaladamente a la "elaboración de perfiles" (Art. 21).

De un modo indirecto, los "Principios" de «limitación de la finalidad», de «minimización de datos» y de «limitación del plazo de conservación» (Art. 5 1 b), c) y e), además del "Derecho de supresión («el derecho al olvido»)" (Art. 17), imponen una limitación importante a la colecta y conservación de datos, necesarias para la efectividad de los algoritmos basados en el aprendizaje automático [machine learning].

---

[136] Se trata del Reglamento (UE) 2019/881, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a *la certificación de la ciberseguridad de las tecnologías de la información y la comunicación* y por el que se deroga el Reglamento (UE) n.º 526/2013.

[137] El *Informe* está disponible, pero solamente en inglés. Mientras tanto, la Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre *la inteligencia artificial en la era digital* (2020/2266(INI)) nos faculta un ponto de situación oficial, más allá de las "filtraciones de prensa".

[138] Como la Comisión Europea puso de manifiesto en sus Comunicaciones *Hacia una economía de los datos próspera* (COM(2014) 0442 final, de 2 de julio) y *Una Estrategia para el Mercado Único Digital de Europa* (COM(2015) 192 final, de 5 de mayo), desde las perspectivas de la protección de los consumidores y de la defensa de competencia.

Esto, sin olvidar las correspondientes "obligaciones del responsable del tratamiento" (Art. 24 y 25), como la de realizar "evaluaciones de impacto" antes del tratamiento por sistemas de IA, ya que estos conllevan "un alto riesgo para los derechos y libertades de las personas físicas", como ocurre en caso de "evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar" (Art. 35 1 y 3 a).

Más allá de la protección de datos, la primera iniciativa correspondió al Parlamento Europeo, con la Resolución de 16 de febrero de 2017 con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL))[139].

Por su parte y a través de Comunicaciones sucesivas, la Comisión Europea puso en marcha un procedimiento destinado a concretar paulatinamente políticas y reglas específicas para enmarcar la utilización de sistemas de IA en la Unión Europea.

Señaladamente, tal se dio con Comunicación Inteligencia artificial para Europa (COM(2018) 237 final, de 25 de abril), en articulación con la, más general, Hacia un espacio común europeo de datos (COM(2018) 232 final, de la misma fecha). Ese mismo año y con un objetivo más práctico, se publicó el primer Plan coordinado sobre la inteligencia artificial (COM(2018) 795 final, de 7 de diciembre), destinado a concretar caminos comunes de investigación, desarrollo e inversiones por parte de la Unión Europea y los Estados-Miembros.

El paso siguiente se planteó con la Comunicación Generar confianza en la inteligencia artificial centrada en el ser humano (COM(2019) 168 final, de 8 de abril), la cual ha tenido un especial relieve al estar basada y recibir las Directrices éticas para una IA fiable, presentadas por el Grupo independiente de expertos de alto nivel sobre inteligencia artificial, creado por la Comisión Europea em junio de 2018.

La consolidación de las aportaciones se dio con el Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza (COM(2020) 65 final, de 19 de febrero), destinado a un debate amplio con todos los interesados, culminando con la Comunicación Fomentar un planteamiento europeo en materia de inteligencia artificial, la cual enmarcó la Propuesta de qua.

Por otra parte y mientras tanto, en lo que se refiere a los derechos de los consumidores y a la regulación de la competencia las respuestas tardaron. Solamente llegando con la Directiva (UE) 2019/2161, de 27 de noviembre, por la que se modifican las Directivas 93/13/CEE, Directivas 98/6/CE, 2005/29/CE y 2011/83/UE, en lo que atañe a la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la Unión. Con esta, se impuso la transparencia algorítmica en la clasificación de ofertas comerciales dentro de los resultados de las búsquedas en línea o en la personalización de precios en resultado de toma de decisiones automatizada, además de en lo que atañe a la elaboración de perfiles del comportamiento de los consumidores (Arts. 5 y 7)

Por último, las Propuestas de Reglamento de relativo a un mercado único de servicios digitales (Ley de servicios digitales [DSA]) y sobre mercados disputables y

[139] Esta *Resolución* se basó en el *Informe* redactado bajo responsabilidad, y el empuje, de la Diputada luxemburguesa Mady Delvaux.

equitativos en el sector digital (Ley de Mercados Digitales [DMA]) (COM(2020) 825 final y COM(2020) 842 final, de 15 de diciembre)[140], las cuales buscan responder a los retos que resultan de los sistemas de IA en lo que se refiere a la elaboración de perfiles y al seguimiento de los consumidores, pero también en lo relativo a la reversibilidad de la anonimización (Arts. 14 6., 15 2. c), 29 1. y 30 de DSA y Arts. 3 6. c) y 5. a) y 13 del DMA).

3. El contexto global

A lo sumo, la Unión Europea está concretizando en forma de ley los Principios éticos relativos a los sistemas de IA, sobre los cual incluso existe una gran convergencia, incluso multicivilizacional.

De hecho y si nos fijamos en iniciativas con especial interés para México, debemos señalar la Recomendación sobre los Principios de la Inteligencia Artificial (C/MIN(2019)3/FINAL), del Consejo de ministros de la OCDE – Organización para la Cooperación y el Desarrollo Económicos, de 22 de mayo de 2019[141].

Pocas semanas después, además de constar como referencia en la Declaración de los Lideres, acordada en la 14ª Cumbre del G20, de 9 de junio de 2019, en Osaka, Japón, la Declaración Ministerial sobre Comercio y Economía Digital, cuenta con un Anexo recibiendo los Principios de la OCDE.

En la misma dirección, tenemos los Principios presentes en el Llamamiento de Roma para la ética de la Inteligencia Artificial,[142], firmados por el Vaticano, la FAO – Organización de las Naciones Unidas para la Alimentación y la Agricultura y Big Techs, como IBM o Microsoft, en 28 de febrero de 2020. Con ello, se busca la construcción de una "algor-ética", una Ética de los algoritmos, delineada por la Pontificia Academia para la Vida, siguiendo el magisterio del Papa Francisco y teniendo como referencia la Declaración Universal de Derechos Humanos, más allá de la Doctrina de la Iglesia Católica.

Terminamos mencionando a un instrumento con un contenido más elaborado, la Recomendación sobre la Ética de la Inteligencia Artificial (SHS/BIO/REC-AIETHICS/2021) de UNESCO, la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, aprobada el 23 de noviembre de 2021, por su 41ª Conferencia General[143]. La Recomendación está estructurada en Valores y Principios, además de Ámbitos de Acción Política, todos ellos muy detallados y abarcando cuestiones que sobrepasan en mucho el ámbito de UNESCO como agencia especializada de Naciones Unidas.

Sin embargo, todos y cada uno de estos marcos se mantiene en las dimensiones ética y política, sin un carácter vinculante. Al paso que la Unión Europea está haciendo lo más difícil, aprobar legislación apta a enmarcar tecnologías que se están haciendo vitales para las personas, para las empresas e incluso para los Estados.

---

[140] Mientras tanto, ya se lograron los acuerdos políticos, entre el Parlamento Europeo y el Consejo, relativos a la *Ley de Servicios Digitales* <https://www.consilium.europa.eu/es/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/> y la *Ley de Mercados Digitales* <https://www.consilium.europa.eu/es/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/>. Accesos em 31/07/2022.

[141] Además, la OCDE ha creado un *Observatorio sobre Políticas de IA* de los Estados-Miembros <https://oecd.ai/en/>. Acceso en 31/07/2022.

[142] Esta iniciativa tiene una página propia, pero solo en inglés <https://www.romecall.org/>. Acceso en 31/07/2022

[143] La *Recomendación* y demás documentación de UNESCO sobre IA, se encuentran disponibles también en español <https://es.unesco.org/artificial-intelligence/ethics>. Acceso en 31/07/2022.

Referencias

COMISIÓN EUROPE. A. Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Hacia una economía de los datos próspera (COM(2014) 0442 final, de 2 de julio). Disponible em https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52014DC0442
Acceso en 31/07/2022.

COMISIÓN EUROPEA. Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Una Estrategia para el **Mercado Único Digital de Europa** (COM(2015) 192 final, de 5 de mayo). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52015DC0192
Acceso en 31/07/2022.

COMISIÓN EUROPEA. Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Inteligencia artificial para Europa (COM(2018) 237 final, de 25 de abril). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0237
Acceso en 31/07/2022.

COMISIÓN EUROPEA. Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Hacia un espacio común europeo de datos (COM(2018) 232 final, de 25 de abril). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0232
Acceso en 31/07/2022.

COMISIÓN EUROPEA. Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Plan coordinado sobre la inteligencia artificial (COM(2018) 795 final, de 7 de diciembre). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0795
Acceso en 31/07/2022.

COMISIÓN EUROPEA. Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Generar confianza en la inteligencia artificial centrada en el ser humano (COM(2019) 168 final, de 8 de abril). Disponible em https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52019DC0168
Acceso en 31/07/2022.

COMISIÓN EUROPEA. Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza (COM(2020) 65 final, de 19 de febrero). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0065
Acceso en 31/07/2022.

COMISIÓN EUROPEA. Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE (COM(2020) 825, de 15 de diciembre). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0825
Acceso en 31/07/2022**.**

COMISIÓN EUROPEA. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales) (COM(2020) 842, de 15 de diciembre). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0842
Acceso en 31/07/2022.

COMISIÓN EUROPEA. Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Brújula Digital 2030: el enfoque de Europa para el Decenio Digital (COM(2021) 118 final, de 9 de marzo). Disponible en

https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021DC0118 Acceso en 31/07/2022.

COMISIÓN EUROPEA. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas em materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. (COM(2021) 206 final, de 21 de abril). Disponible en https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF Acceso en 31/07/2022.

COMISIÓN EUROPEA. Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Fomentar un planteamiento europeo en materia de inteligencia artificial (COM(2021) 205 final, de 21 de abril). Disponible em https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021DC0205 Acceso en 31/07/2022.

COMISIÓN EUROPEA. Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a las máquinas y sus partes y accesorios (COM(2021) 202 final, de 21 de abril), también con anexos. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021PC0202 Acceso en 31/07/2022.

CONSEJO DE MINISTROS DE LA UNIÓN EUROPEA. Conclusiones de la Presidencia La Carta de los Derechos Fundamentales en el contexto de la inteligencia artificial y el cambio digital (11481/20, de 21 de octubre). Disponible en https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/es/pdf Acceso en 31/07/2022.

COTINO HUESO, LORENZO. Un análisis crítico constructivo de la Propuesta de Reglamento de la Unión Europea por el que se establecen normas armonizadas sobre la Inteligencia Artificial (Artificial Intelligence Act). DIARIO LA LEY, 26/06/2021 (ISSN: 1989-6913). Disponible en https://diariolaley.laleynext.es/dll/2021/07/02/un-analisis-critico-constructivo-de-la-propuesta-de-reglamento-de-la-union-europea-por-el-que-se-establecen-normas-armonizadas-sobre-la-inteligencia-artificial-artificial-intelligence-act
Acceso en 31/07/2022.

DE MIGUEL ASENSIO, Pedro A. Propuesta de Reglamento sobre Inteligencia Artificial. La Ley – Unión Europea, 2021, 92 (ISSN: 255-551X). Disponible en https://eprints.ucm.es/id/eprint/65870/1/PADemiguelAsensio%20LaLey%20UE%20n%2092%2005.21.pdf Acceso en 31/07/2022.

GARCÍA GARCÍA, Sara. Una aproximación a la futura regulación de la inteligencia artificial en la Unión Europea. Revista de Estudios Europeos, 2022, 79, pp. 304-323. (ISSN: 2530-9854). Disponible em https://uvadoc.uva.es/bitstream/handle/10324/53218/revistas_uva_es__ree_article_view_5728_4204.pdf Acceso en 31/07/2022.

G20. ANNEX to the Ministerial Statement on Trade and Digital Economy. Aprobado en 8 y 9 de junio de 2019. Disponible en https://www.mofa.go.jp/files/000486596.pdf Acceso en 31/07/2022.

GRUPO INDEPENDIENTE DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL. Directrices éticas para una IA fiable. Disponible en https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-es/format-PDF
Acceso en 31/07/2022.

OCDE – ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS. Recomendación del Consejo de ministros sobre los Principios de la Inteligencia Artificial (C/MIN(2019)3/FINAL, de 22 de mayo de 2019) [Versiones oficiales, solamente en inglés y francés]. Disponible en https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
Acceso en 31/07/2022

PARLAMENTO EUROPEO. Resolución con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL), de 16 de febrero de 2017). Disponible en https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html Acceso en 31/07/2022.

PARLAMENTO EUROPEO. Resolución sobre el Marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL), de 20 de octubre). Disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.html Acceso en 31/07/2022.

PARLAMENTO EUROPEO. Resolución sobre la inteligencia artificial en la era digital (2020/2266(INI), de 3 de mayo de 2022). Disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_ES.html Acceso en 31/07/2022.

PARLAMENTO EUROPEO (Comisión de Asuntos Jurídicos). Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica. ((2015/2103(INL), de 27 de enero de 2017). Disponible en https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.html Acceso en 31/07/2022.

PARLAMENTO EUROPEO (Comisión Especial sobre Inteligencia Artificial en la Era Digital). Informe sobre la Inteligencia Artificial en la Era Digital (2020/2266(INI), de 3 de mayo de 2022). Disponible em https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2266(INI)&l=es Acceso en 31/07/2022.

UNIÓN EUROPEA. Tratados vigentes (Versiones consolidadas, incluyendo la Carta de los Derechos Fundamentales de la Unión Europea). Disponibles en https://eur-lex.europa.eu/collection/eu-law/treaties/treaties-force.html?locale=es Acceso en 31/07/2022.

UNIÓN EUROPEA. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en https://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=celex:31995L0046 Acceso en 31/07/2022.

UNIÓN EUROPEA. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679
Acceso en 31/07/2022.

UNIÓN EUROPEA. Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013. Disponible em https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32019R0881 Acceso en 31/07/2022.

UNIÓN EUROPEA. Directiva del Parlamento Europeo y del Consejo (UE) 2019/2161, de 27 de noviembre, por la que se modifican las Directivas 93/13/CEE, Directivas 98/6/CE, 2005/29/CE y 2011/83/UE, en lo que atañe a la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la Unión. Disponible em https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32019L2161 Acceso en 31/07/2022.

Por Que Confiar Na Autoridade Nacional De Proteção De Dados?

Leonardo Parentoni[144]

RESUMO

A Autoridade Nacional de Proteção de Dados (ANPD), principal órgão regulador do microssistema brasileiro de proteção de dados pessoais, surgiu cercada de muitas expectativas, mas também de fundadas dúvidas acerca de sua real capacidade para regular o sistema de maneira satisfatória, condizente com as referidas expectativas e com o importantíssimo papel que lhe fora atribuído pela Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018 – LGPD). O método utilizado na pesquisa foi a análise estruturalista da ANPD (comparando estrutura e função das instituições), valendo-se também de breve incursão no Direito comparado para analisar as semelhanças entre a ANPD e instituições estrangeiras de papel semelhante, constituídas há mais tempo, a fim de demonstrar que a estrutura atual da ANPD, por si só, não seria empecilho ao bom exercício de suas funções. Realizou-se, portanto, uma pesquisa qualitativa e comparativa, com foco na estrutura das autoridades nacionais de proteção de dados. Na sequência, o texto traz um levantamento das principais ações realizadas pela ANPD até abril de 2021, com análise crítica de três delas. Ao final, concluiu-se que a estrutura inicial da ANPD, conquanto não seja considerada a ideal pelos estudiosos da matéria, ao menos até o momento, não vem sendo obstáculo para que essa autoridade reguladora desempenhe satisfatoriamente as suas funções e corresponda à enorme expectativa criada ao seu redor, ainda que alguns pontos de suas primeiras ações sejam tecnicamente discutíveis, como demonstrado ao longo do texto. Algo que poderia ocorrer também com qualquer outra autoridade reguladora, inclusive com aquelas já constituídas e estabilizadas há décadas, pois pequenas divergências são naturais.

PALAVRAS-CHAVE:

Privacidade. Proteção de Dados Pessoais. Lei Geral de Proteção de Dados Pessoais (LGPD). Autoridade Nacional de Proteção de Dados (ANPD). Autoridade Uruguaia de Proteção de Dados (URCDP).

---

[144] **Leonardo Parentoni** tem mais de 20 anos de experiência nos setores público e privado. Membro do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade no Brasil - CNPD. É Doutor em Direito pela USP. Mestre em Direito Empresarial pela UFMG. Procurador Federal/AGU. Professor da UFMG e do IBMEC/MG. Fundador e Conselheiro Científico do Centro de Pesquisa em Direito, Tecnologia e Inovação – DTIBR (www.dtibr.com). Fundador e Coordenador da área de concentração em Direito, Tecnologia e Inovação na Pós-Graduação da Faculdade de Direito da UFMG. Ex-membro de Comissões do Conselho Nacional de Justiça, do Conselho da Justiça Federal, da Procuradoria-Geral Federal e da OAB/MG. Pesquisador Visitante na Universidade do Texas em Austin/USA e na Agência de Proteção de Dados do Uruguai. Parceiro tecnológico estratégico na Universidade de Tecnologia de Sydney. Mentor de Equipe no Programa Law Without Walls – LWOW/USA. Principais áreas de atuação: 1) Direito, Tecnologia e Inovação; 2) Direito Societário; 3) Análise Empírica do Direito (*Empirical Legal Studies - ELS*). Número de Identificação como Pesquisador Internacional (*Researcher ID*): N-5627-2015. Publicações disponíveis gratuitamente em: https://www.researchgate.net/profile/Leonardo-Parentoni Currículo Lattes completo em Português e Inglês disponível em: http://lattes.cnpq.br/3612200644224606

Why Trust The Brazilian Data Protection Authority?

Leonardo Parentoni

ABSTRACT

The Brazilian Data Protection Authority (ANPD), the main public regulatory body of the local data protection legal system, emerged surrounded by high expectations, but also by well-grounded doubts about its real capacity to satisfactorily regulate that system, according to the aforementioned expectations and fulfilling the important role that the Brazilian Data Protection Act (Act number 13,708/2018) has assigned to it. The author of this article has performed a structuralist analysis of the ANPD, also using comparative law to identify similarities between the ANPD and foreign institutions with the same role and powers, aiming at demonstrating that the actual structure of ANPD, by itself, would not hinder the proper performance of its duties. Thus, the author performed both qualitative and comparative research, focusing on the structure of the national data protection authorities. Next, the article provides a survey of the main measures carried out by the Brazilian Data Protection Authority until April 2021, critically assessing three of them. In the end, the conclusion showcases that the initial structure of ANPD, although not the ideal structure as desired by scholars of the field, at least so far has not hindered that public regulatory body from satisfactorily fulfilling its duties and corresponding to the enormous expectation related to it. Nevertheless, some parts of its first measures are technically debatable, as shown throughout the text. Something that could also happen with any public regulatory body, even with those already in place for decades, since small divergences are natural.

KEYWORDS:

Privacy. Personal Data Protection. The Brazilian Data Protection Act (LGPD). The Brazilian Data Protection Authority (ANPD). The Uruguayan Data Protection Authority (URCDP).

1. INTRODUÇÃO: PROCESSO LEGISLATIVO DE CRIAÇÃO DA ANPD E DO CNPD

A Autoridade Nacional de Proteção de Dados (ANPD), principal órgão regulador do microssistema brasileiro de proteção de dados pessoais, surgiu cercada de muitas expectativas, após um longo e tumultuado processo legislativo, cheio de "altos e baixos". Como se demonstrará a seguir, de forma muito breve, diversas razões convergiram para que o formato final da ANPD fosse muito diferente daquele desejado pelos estudiosos da área.

Com efeito, a criação da ANPD não estava prevista na redação original do Projeto de Lei n. 4.060/2012[145], o qual, anos depois, veio a se tornar a LGPD (Lei n. 13.709/2018). Sua primeira previsão constou do Projeto de Lei n. 5.276/2016 (art. 53)[146], no qual foi estruturada como órgão público, ou seja, de modo semelhante ao seu formato atual. Ocorre que, ainda durante a tramitação legislativa deste projeto, de autoria do Poder Executivo, uma emenda parlamentar alterou o formato para autarquia[147], nos termos do art. 55 do PLC n. 53/2018, ao argumento de que somente nesse novo formato a ANPD teria independência para bem desempenhar as suas funções. Como será abordado no texto, tal formato é considerado o ideal por muitos estudiosos do tema.

É bom recordar que, nessa época (anos de 2016 a 2018), o Brasil experimentou crise econômica e instabilidade política, tendo ocorrido o impeachment da Presidente Dilma Rousseff e a posse de Michel Temer, que a substituiu nas funções. Neste contexto, o Presidente Temer considerou que inadequado criar um ente público sob a forma de autarquia, pois isto implicaria aumento de despesas para o Estado, indo na contramão das medidas de austeridade fiscal que estavam sendo praticadas pelo governo. O Presidente então vetou a criação da ANPD[148], ao fundamento de que seria inconstitucional emenda parlamentar impor aumento de despesas em projeto de lei de iniciativa do Poder Executivo, conforme art. 63, I da Constituição de 1988, que haveria usurpação de atribuição privativa do Presidente, prevista no art. 61, § 1º, II, "e" da

---

145 BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4.060/2012**. Disponível em <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 17 ago. 2021. DONEDA, Danilo Cesar Maganhoto. Rumo à Autoridade Nacional de Proteção de Dados. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coord.). **Direito & Internet IV**: Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019. p. 480. "O texto enviado pelo poder executivo ao parlamento, no entanto, não compreendia a criação de uma autoridade para supervisionar a aplicação da lei. A pertinência de sua criação, embora reconhecida e debatida amplamente nos debates públicos realizados pelo Ministério da Justiça, não resultou em um texto que compreendesse a criação do órgão, dado ao fato de não haver uniformidade de entendimento em relação à matéria à época no executivo federal. Ainda assim, pode-se afirmar que o texto enviado reconhecia de forma implícita a centralidade de um órgão especializado para a aplicação da legislação de proteção de dados, ao se referir por dezenas de vezes a um 'órgão competente' para a funcionalização de muitos de seus ditames e garantias e propondo mecanismos de tutela que, para serem materialmente viáveis e factíveis, dependeriam da atuação deste órgão. Ainda assim, pelos motivos mencionados, o texto não faz aceno a nenhum aspecto constitutivo deste órgão nem associa as suas funções a qualquer entidade então já existente."

146 BRASIL. Câmara dos Deputados. **Projeto de Lei nº 5.276/2016**. Disponível em <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 17 ago. 2021.

147 O art. 5º, I do Decreto-lei n. 200/1967 definiu autarquia como "o serviço autônomo, criado por lei, com personalidade jurídica, patrimônio e receita próprios, para executar atividades típicas da Administração Pública, que requeiram, para seu melhor funcionamento, gestão administrativa e financeira descentralizada".

148 BRASIL. Presidência da República. **Mensagem de Veto n. 451/2018**. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm>. Acesso em: 17 ago. 2021.

Constituição e porque a matéria demandaria lei específica, conforme art. 37, XIX do texto constitucional. Houve quem questionasse a tecnicidade do veto. Por exemplo, o ex-Ministro do STF, Ilmar Galvão, defendeu a constitucionalidade da criação da ANPD por emenda parlamentar[149]. Mas fato é que o veto foi mantido e a LGPD foi publicada em 14 de agosto de 2018, sem prever a criação da ANPD.

Evidentemente, numa matéria tão complexa e cercada de expectativas, a existência de autoridade reguladora é peça-chave. Por isso, ainda no mesmo ano, em 27 de dezembro de 2018, o próprio Poder Executivo apresentou a Medida Provisória n. 869/2018, que realizou alguns ajustes pontuais na LGPD, mas cujo principal objetivo foi a criação da ANPD, estruturada como órgão público[150], sem aumento de despesa (art. 55-A), tal como já havia sido originalmente delineado em 2016[151]. Reacendeu-se então o debate sobre esse modelo, com ampla participação da sociedade civil, imprensa e estudiosos da matéria[152]. O que mais chamava a atenção era o receio de que, por estar formalmente vinculada ao Poder Executivo, a ANPD não apresentasse a necessária independência para exercer suas funções[153]. Este aspecto se acentuou em 18 de junho de 2019, quando, antes mesmo de ser concluída a tramitação legislativa da MP n. 869/2018, sobreveio a Lei n. 13.844/2019, cujos artigos art. 2º, VI e 12 inseriram formalmente a ANPD na estrutura da Presidência da República. Este formato se consolidou em 08 de julho de 2019, com a conversão da MP n. 869/2018 na Lei n. 13.853/2019. É esta, portanto, a estrutura atual da ANPD.

O intenso debate travado à época evidenciou que essa estrutura, conquanto não seja a ideal, era a possível, tendo em vista, sobretudo, o contexto de crise econômica[154], que se agravou ainda mais com a pandemia de SARS-CoV 2 (Covid-

---

[149] JOTA. **Ex-Ministro diz que não há vício de inconstitucionalidade na criação da ANPD**. São Paulo: 31 jul. 2018. Disponível em <https://www.jota.info/docs/ex-ministro-diz-que-nao-ha-vicio-de-inconstitucionalidade-na-criacao-da-anpd-31072018>. Acesso em: 17 ago. 2021.

Vide também: PFEIFFER, Roberto Augusto Castellanos. A Saga da Autoridade Nacional de Proteção de Dados: Do veto à Lei nº 13.853/2019. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coord.). **Direito & Internet IV**: Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019. p. 454. "Como a Medida Provisória nº 869/2018, veiculada em instrumento normativo de uso exclusivo do Presidente da República tinha como objetivo central precisamente a criação da ANPD, não mais subsistia tal impedimento. Assim, a modificação da natureza da autoridade durante a tramitação legislativa não significaria afronta ao 61, § 1º, II, 'e' da Constituição Federal.

E como a institucionalização da ANPD com a natureza de órgão da administração indireta seria advinda da conversão da Medida Provisória nº 869/2018 em lei, estaria suprido também o requisito de criação de autarquia mediante lei específica, cumprindo-se assim o comando do art. 37, XIX da Constituição Federal."

[150] Portanto, sem personalidade jurídica, sem garantias orçamentárias e desprovida de carreira de apoio específica.

[151] Op. cit. p. 455. "A distinção de natureza é muito impactante: enquanto a autarquia especial possui autonomia administrativa, financeira e hierárquica, o órgão da administração direta é destituído de tais características, tendo em vista a sua subordinação hierárquica."

[152] SILVA, Victor Hugo. **Autoridade Nacional de Proteção de Dados é criada por Medida Provisória**. São Paulo: 28 dez. 2018. Disponível em: <https://tecnoblog.net/273018/mp-autoridade-nacional-protecao-dados/>. Acesso em: 17 ago. 2021.

[153] VASCONCELOS, Beto; DE PAULA, Felipe. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais**: e suas repercussões no Direito Brasileiro. São Paulo: Revista dos Tribunais, 2019. p. 735. "É, portanto, de elevado risco regulatório a instituição de uma ANDP com estrutura reduzida, criada sob o enunciado político de ausência de 'aumento de despesa', com comando de regulação de 'intervenção mínima', desenhada para ter limitada autonomia e independência técnica, administrativa e financeira, seja com relação aos agentes privados regulados, mas, sobretudo, com relação ao Poder Público."

[154] PARENTONI, Leonardo. Autoridade Nacional de Proteção de Dados Brasileira: Uma visão otimista. **Revista do Advogado**. São Paulo: AASP, Ano XXXIX, n. 144, p. 209-219, nov. 2019. p. 211. "Tem-se plena consciência de que esse não é o modelo ideal, mas sim o modelo possível no atual contexto do país."

19)[155]. Na contramão das críticas, houve quem destacasse que essa estrutura inicial não seria empecilho ao bom desempenho das funções da ANPD, dando-lhe um voto de confiança[156]. Da mesma forma, a Lei n. 13.853/2019 inseriu na LGPD o art. 55-A, §§ 1º e 2º, prevendo textualmente que essa estrutura é transitória e deverá ser reavaliada após 02 anos, para eventualmente transformá-la em autarquia especial.

Neste ponto, o leitor mais atento já deve estar se perguntando se a mencionada revisão já foi feita, pois o prazo de 02 anos teria se encerrado em dezembro de 2020. Ocorre que os citados dispositivos da LGPD fixaram que a revisão ocorreria em 02 anos contados da "entrada em vigor da estrutura regimental da ANPD". Sendo que a estrutura regimental foi definida pelo Decreto n. 10.474/2020, cujo art. 6º dispôs que "este Decreto entra em vigor na data de publicação da nomeação do Diretor-Presidente da ANPD no Diário Oficial da União". O que somente veio a ocorrer em 06 de novembro de 2020[157]. Esta, portanto, é a data oficial de início de funcionamento da autoridade. Consequentemente, a revisão estrutural está prevista para ocorrer até novembro de 2022.

Fato é que, apesar de formalmente criada pela MP n. 869/2018, em 27 de dezembro de 2018, a ANPD somente começou a operar, de fato, em 06 de novembro de 2020, quando foram empossados os seus primeiros diretores. E, mesmo nessa data, sua estruturação ainda não estava completa, uma vez que o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), importante órgão consultivo previsto nos artigos 58-A e 58-B da LGPD, somente teve os seus primeiros membros designados em 09 de agosto de 2021[158]. Ou seja, da criação formal da ANPD até o efetivo preenchimento de sua estrutura interna transcorreram quase 03 anos.

Encerra-se esta breve contextualização histórica destacando que em 13 de junho de 2022 foi apresentada, pelo Presidente da República, a Medida Provisória n. 1.124 que propõe, logo em seu artigo 1º, transformar a ANPD em autarquia de natureza especial, de modo a superar, ao menos em tese, alguns dos óbices à atuação dessa autoridade reguladora, conforme abordado neste tópico. Se haverá a conversão da medida provisória em lei, se ela perderá eficácia, ou quais serão as possíveis emendas apresentadas no Congresso Nacional, é algo que só o tempo irá dizer.

---

[155] BRASIL. Agência Brasil. **Desemprego registrou taxa média de 13,5% em 2020**. Brasília: 10 mar. 2021. Disponível em <https://agenciabrasil.ebc.com.br/economia/noticia/2021-03/desemprego-registrou-taxa-media-de-135-em-2020>. Acesso em: 17 ago. 2021.

[156] PARENTONI, Leonardo. Autoridade Nacional de Proteção de Dados Brasileira: Uma visão otimista. **Revista do Advogado**. São Paulo: AASP, Ano XXXIX, n. 144, p. 209-219, nov. 2019. p. 217. Disponível em <https://www.researchgate.net/publication/337740878_Autoridade_Nacional_de_Protecao_de_Dados_Brasileira_Uma_visao_otimista_Brazilian_National_Data_Protection_Authority_An_optimistic_view>. Acesso em: 17 ago. 2021. "É inequívoco que a ANPD não tem a estrutura ideal, desejada por seus idealizadores e inspirada no modelo europeu. Por esta razão, vem recebendo severas críticas, como se estivesse fadada ao fracasso. O presente texto pretendeu fornecer visão diferente e mais otimista, demonstrando que a ANPD já possui garantias suficientes para uma atuação independente. Sendo assim, seu efetivo êxito dependerá mais da habilidade dos primeiros Diretores do que da estrutura estaticamente prevista em lei."

[157] Os primeiros diretores da ANPD foram escolhidos pelo Presidente da República por meios das Portarias n. 614 a 618, publicadas no DOU em 15.10.2020, cujos nomes foram, na sequência, remetidos ao Senado Federal, para "sabatina". A aprovação destes nomes pelo Senado e a efetiva posse dos diretores, incluindo o Diretor-Presidente, ocorreu por meio do Decreto não numerado, de 05.11.2020, publicado no DOU no dia seguinte, ou seja, em 06.11.2020.

[158] BRASIL. Autoridade Nacional de Proteção de Dados. **Presidente da República designa membros do CNPD**. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/noticias/presidente-da-republica-designa-membros-do-cnpd>. Acesso em: 17 ago. 2021.

2. OS VÁRIOS FORMATOS DAS AUTORIDADES NACIONAIS DE PROTEÇÃO DE DADOS

É tradicional que um sistema de proteção de dados pessoais compreenda uma autoridade reguladora[159], responsável por supervisionar esta matéria[160]. Ela pode se estruturar de várias formas diferentes[161], sem que isto comprometa o exercício de suas funções[162]. Tanto que a Convenção 108/1981 do Conselho da Europa[163] – primeiro tratado internacional vinculante sobre proteção de dados – exigia que os Estados signatários se comprometessem a adotar uma série de padrões mínimos, mas não impôs qualquer formato para as autoridades reguladoras, o que reforça o argumento de que existe mais de uma forma de se alcançar bom resultado.

Nos Estados Unidos da América não existe sequer autoridade reguladora específica, dedicada exclusivamente à proteção de dados pessoais. Essa função é exercida pela Federal Trade Commission – FTC, cumulativamente com várias outras atribuições, inclusive com a sua principal missão, que é a de "proteger os consumidores e a concorrência"[164]. Tanto a FTC atua de forma efetiva que a maior sanção já aplicada no mundo, em decorrência de tratamento indevido de dados pessoais, foi a multa de 05 bilhões de dólares imposta por ela ao Facebook, em 2019[165].

---

[159] Não é o propósito deste breve texto discutir os vários aspectos técnicos do conceito de regulação. A quem se interessar pelo tema, recomenda-se: KOPP, Christel; LODGE, Martin. What is regulation? An interdisciplinary concept analysis. **Regulation & Governance**. Hoboken: Wiley. v. 11, n. 01, p. 01-43, Jul. 2015; e BALDWIN, Robert; CAVE, Martin; LODGE, Martin. **Understanding Regulation**: Theory, Strategy, and Practice. Oxford: Oxford University Press, 2012.

[160] Na tradição europeia, tais instituições são denominadas *data protection authorities* – DPAs.

EUROPEAN COMMISSION. **What are Data Protection Authorities (DPAs)?** Disponível em <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en>. Acesso em: 17 ago. 2021. "DPAs are independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against violations of the General Data Protection Regulation and the relevant national laws. There is one in each EU Member State."

WIMMER, Miriam. Autoridades de Proteção de Dados Pessoais no Mundo: fundamentos e evolução na experiência comparada. *In*: PALHARES, Felipe (Coord.). **Temas Atuais de Proteção de Dados**. São Paulo: Revista dos Tribunais, 2020. p. 154. "As estratégias nacionais para proteção de dados pessoais sofreram mudanças ao longo do tempo, em resposta ao desenvolvimento tecnológico, às novas possibilidades de utilização de dados pessoais e à compreensão jurídica dos direitos associados à proteção de dados não mais apenas como liberdades negativas, mas como direitos dotados de dimensão positiva, necessários para o exercício da autodeterminação informativa e para o exercício das liberdades informacionais. Tais mudanças vieram acompanhadas da crescente relevância atribuída às autoridades de proteção de dados pessoais, entidades compreendidas como elemento-chave das estratégias regulatórias para proteção de direitos do indivíduo na sociedade da informação."

[161] Uma boa fonte de consulta é o censo das autoridades de proteção de dados pessoais periodicamente publicado pela *International Conference of Data Protection & Privacy Commissioners* – ICDPPC.

[162] Graham Greenleaf há muitos anos monitora os sistemas de proteção de dados pessoais de vários países. No relatório de 2021, ele informou que menos de 10% dos 145 Estados analisados estariam desprovidos de autoridade independente: GREENLEAF, Graham. Global data privacy 2021: DPAs joining networks are the rule. *Privacy* **Laws & Business International Report**. London: Privacy Laws & Business. v. 170, n. 01, p. 23-26, Jan. 2021. p. 23. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3874834>. Acesso em: 24 ago. 2021.

[163] CONSELHO DA EUROPA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. Disponível em <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures>. Acesso em: 17 ago. 2021.

[164] UNITED STATES OF AMERICA. **Federal Trade Commission – About the FTC**. Disponível em: <https://www.ftc.gov/about-ftc>. Acesso em: 17 ago. 2021.

[165] UNITED STATES OF AMERICA. **Federal Trade Commission – News & Events**. Disponível em: <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>. Acesso em: 17 ago. 2021.

Modelo oposto se verifica na União Europeia, em que as autoridades reguladoras de proteção de dados pessoais costumam ser estruturadas para tratar especificamente deste tema, havendo previsão legislativa de várias garantias para o seu bom funcionamento. Por exemplo, o Tratado sobre o Funcionamento da União Europeia[166] destaca que esta matéria deverá ficar "sujeita ao controlo de autoridades independentes" (art. 16, 2). Na mesma linha, a Carta dos Direitos Fundamentais da União Europeia[167] (art. 8, 3) afirma ser imprescindível que a supervisão seja realizada "por parte de uma autoridade independente". No modelo europeu, somente se considera independente[168] a autoridade que reúna determinados requisitos, previstos no art. 52 do Regulamento 2016/679 (GDPR), como não se sujeitar a "influências externas, diretas ou indiretas no desempenho das suas funções", dispor "dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessários à prossecução eficaz das suas atribuições", selecionar e dispor "do seu próprio pessoal" (leia-se, carreira de apoio específica) e também "que disponha de orçamentos anuais separados e públicos". Aliás, um dos principais objetivos do citado regulamento foi justamente harmonizar a atuação das autoridades nacionais, fixando requisitos comuns, para minimizar a grande discrepância que existia anteriormente[169].

Por estar estruturada como órgão, ao invés de autarquia, a ANPD não preenche todos esses requisitos. Seu orçamento está atrelado ao da Presidência da República e não há carreira de apoio diferenciada, no sentido de que não há concurso público específico para a seleção dos servidores que nela atuam, ao contrário do que ocorre em algumas autarquias, como INSS e Banco Central.

A ANPD, portanto, não se enquadra perfeitamente no modelo europeu. O que não é surpresa, visto que diversos fatores dificultam replicar esse modelo em nações com cultura e evolução histórica absolutamente diferente, como é o caso do Brasil[170].

---

166 UNIÃO EUROPEIA. **Tratado sobre o Funcionamento da União Europeia**. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012E/TXT>. Acesso em: 17 ago. 2021.

167 UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. Disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT>. Acesso em: 17 ago. 2021.

168 DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção e dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 385-386. "O recurso a uma autoridade administrativa para a proteção dos dados pessoais, no modelo de uma autoridade independente, é uma tendência fortemente enraizada em alguns ordenamentos. Após sua concepção e adoção em países como Alemanha e Suécia, a obrigatoriedade de sua instituição em todos os países-membros da União Europeia (...) transformou-a em característica integrante do chamado 'modelo europeu' de proteção de dados pessoais. Não se trata, entretanto, de um fenômeno circunscrito ao espaço geográfico e político europeu, pois organismos do gênero estão presentes em países como Argentina, Austrália, Canadá, Japão, Israel, Hong Kong, Nova Zelândia e Taiwan."

169 KORFF, Douwe; GEORGES, Marie. **The DPO Handbook**: Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation. Rome: T4Data Programme, 2019. Available at: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9127859>. Access: 05 Jul. 2020. p. 102. "(...) the General Data Protection Regulation (GDPR or 'the Regulation') was adopted, partly because the 1995 Data Protection Directive had not led to a sufficient level of harmonisation of the laws in the Member States; partly in response to the massive expansion in the processing of personal data since the introduction of the 1995 Data Protection Directive; and partly in response to the case-law of the CJEU."

170 WIMMER, Miriam. Autoridades de Proteção de Dados Pessoais no Mundo: fundamentos e evolução na experiência comparada. *In*: PALHARES, Felipe (Coord.). **Temas Atuais de Proteção de Dados**. São Paulo: Revista dos Tribunais, 2020. p. 155. "(...) é preciso ter presente que estruturas institucionais, políticas públicas e ferramentas regulatórias inevitavelmente assumem a coloração das realidades sociais, políticas e econômicas nas quais estão inseridas. Ainda que desenhos jurídicos, regras regulatórias e arranjos institucionais sejam, em certa medida, passíveis de 'exportação', o ambiente no qual tais estruturas estão inseridas é, em geral, impossível de ser replicado. Essa afirmação é particularmente verdadeira no campo

Isso, contudo, não significa que falte independência à ANPD ou que ela seja incapaz de desempenhar adequadamente as suas funções. Repita-se: conquanto muito importante e com certo protagonismo[171], o modelo europeu é um dos possíveis, não é o único. Existe sim orçamento para a ANPD (ainda que modesto, dado o cenário de crise econômica e pandemia de Covid-19), existem sim competentes servidores atuando no órgão. Ademais, o fato de estar formalmente inserida na estrutura da Presidência da República, por si só, não é certeza de que faltará isenção a seus diretores, para atuar de forma alheia a pressões. Como se demonstrará mais adiante, a LGPD cuidou de dotar os diretores de uma série de garantias, justamente para lhes assegurar independência técnica na tomada de decisão. Tais garantias podem até não contemplar todo o rol característico do modelo europeu, mas na visão deste autor são suficientes, ao menos, para dar um voto inicial de confiança à ANPD, até que sua estrutura seja oportunamente reavaliada.

Com efeito, nem toda autoridade de proteção de dados bem sucedida segue fielmente o padrão europeu. Conforme se demonstrou, a FTC adota modelo totalmente diferente, sem que isto tenha comprometido a sua atuação.

Em Israel, por sua vez, a autoridade local (Israeli Privacy Protection Authority – PPA) está inserida na estrutura do Ministério da Justiça. Ela deve publicar relatórios anuais sobre as atividades desempenhadas no exercício anterior, os quais são submetidos à análise crítica de um órgão colegiado composto por professores, profissionais da área e representantes da sociedade civil (The Public Council for Privacy Protection), o qual então encaminha suas observações a uma comissão do Poder Legislativo, encarregada de supervisionar a matéria (Constitution and Law Committee)[172]. Esse formato atípico não impediu que Israel obtivesse reconhecimento da União Europeia, atestando formalmente que o país apresenta garantias semelhantes àquelas então vigentes no modelo europeu[173], o que se formalizou por meio da "decisão de adequação"[174] de 31 de janeiro de 2011.

---

da proteção de dados pessoais, cujos arranjos jurídicos e institucionais foram, especialmente na Europa, profundamente influenciados por fatos históricos."

171 LYNSKEY, Orla. **The Foundations of EU Data Protection Law**. Oxford: Oxford University Press, 2015. p. 41. "Data protection is one of the rare fields in which the EU could be said to exercise global regulatory supremacy; the EU rules have now been used as a blueprint for regulatory regimes across the Western world."

172 ISRAEL. **Privacy Protection Authority**. About PPA. Disponível em <https://www.gov.il/en/departments/units/privacy_protection_council >. Acesso em: 20 ago. 2021.

173 TIKKINEN-PIRI, Christina; ROHUNEN, Anna; MARKKULA, Jouni. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. **Computer Law & Security Review**. Amsterdam: Elsevier. v. 34, n. 01, p. 134-153, Feb. 2018. p. 145. "The GDPR builds on DIR95 regarding the European Commission's possibility to make an adequacy decision about the level of data protection of a third country (or a territory or a processing sector in that country) or an international organisation. To make the decision, the commission has to assess the level of protection regarding the rule of law, the independent supervisory authority and the international commitments entered into by the third country or the international organisation. (…) If an adequacy decision has been made, a transfer may take place, and any further authorisation to transfer is not required from the supervisory authority."

No mesmo sentido: SARMENTO E CASTRO, Catarina. **Direito da Informática, Privacidade e Dados Pessoais**. Coimbra: Almedina, 2005. p. 281. "A transferência de dados pessoais para países terceiros que assegurem um nível de protecção adequado poderá ser realizada sem outras especiais garantias, uma vez que tal nível de protecção permite que se cumpram os requisitos gerais de protecção de dados exigidos no quadro comunitário."

174 UNIÃO EUROPEIA. Comissão Europeia. **Decisão de Execução da Comissão**. Bruxelas: 31 jan. 2011. Disponível em <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AL%3A2011%3A027%3A0039%3A0042%3Aen%3APDF>. Acesso em: 22 ago. 2021. "Article 1. For the purposes of Article 25(2) of Directive 95/46/EC, the State of Israel

Na própria América do Sul, a autoridade de proteção de dados do Uruguai[175] apresenta estrutura deveras semelhante à da ANPD. É, portanto, um bom parâmetro de comparação, apesar das inegáveis diferenças entre esses dois países com relação ao idioma, extensão territorial, população, PIB, etc.

A autoridade uruguaia denomina-se Unidad Reguladora y de Control de Datos Personales (URCDP)[176]. Ela foi criada pela Ley n. 18.331, de 11 de agosto de 2008, como autoridade central do sistema de proteção de dados pessoais daquele país[177]. Em pouco mais de uma década de funcionamento, já alcançou resultados expressivos, inclusive no plano internacional. Note-se que sua nomenclatura optou por utilizar a expressão "unidade" ao invés de "autoridade", como é tradicional no modelo europeu e utilizado na ANPD. Ou seja, ainda que o nome de uma instituição, por si só, não seja parâmetro para análise estruturalista[178], a diferença entre a URCPD e o modelo europeu começa já a partir daí. A URCDP não está estruturada de maneira semelhante a uma autarquia em regime especial. Pelo contrário, ela é um órgão público inserido na estrutura da Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento – Agesic, instituição responsável por capitanear as ações para o desenvolvimento tecnológico do Uruguai[179]. Por sua vez, a Agesic é uma "uma unidade executora com autonomia técnica, dependente da Presidência da República Oriental

is considered as providing an adequate level of protection for personal data transferred from the European Union (...)."

175 As linhas seguintes trazem um resumo dos argumentos desenvolvidos no pioneiro estudo brasileiro que, após uma estadia de pesquisa *in loco* no Uruguai, em julho de 2019, comparou a estrutura da autoridade reguladora local com a da ANPD. O referido estudo deu origem à seguinte publicação: PARENTONI, Leonardo. Autoridade Nacional de Proteção de Dados Brasileira: Uma visão otimista. **Revista do Advogado**. São Paulo: AASP, Ano XXXIX, n. 144, p. 209-219, nov. 2019. p. 217. Disponível em <https://www.researchgate.net/publication/337740878_Autoridade_Nacional_de_Protecao_de_Dados_Brasileira_Uma_visao_otimista_Brazilian_National_Data_Protection_Authority_An_optimistic_view>. Acesso em: 17 ago. 2021.

176 URUGUAY. **Unidad Reguladora y de Control de Datos Personales – URCDP**. Disponível em <https://www.gub.uy/unidad-reguladora-control-datos-personales/>. Acesso em: 18 ago. 2021.

177 Ley n. 18.331/2008. Art. 31. "CAPITULO VII - ORGANO DE CONTROL. Artículo 31. Organo de Control. - Créase como órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), dotado de la más amplia autonomía técnica, la Unidad Reguladora y de Control de Datos Personales. Estará dirigida por un Consejo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que por sus antecedentes personales, profesionales y de conocimiento en la materia aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos.

A excepción del Director Ejecutivo de la AGESIC, los miembros durarán cuatro años en sus cargos, pudiendo ser designados nuevamente. Sólo cesarán por la expiración de su mandato y designación de sus sucesores, o por su remoción dispuesta por el Poder Ejecutivo en los casos de ineptitud, omisión o delito, conforme a las garantías del debido proceso. Durante su mandato no recibirán órdenes ni instrucciones en el plano técnico."

178 A respeito das análises estruturalista e funcional, consulte-se: BOBBIO, Norberto. **Da Estrutura à Função**: Novos Estudos de Teoria do Direito. Tradução: Daniela Beccaccia Versiani. Barueri: Manole, 2007.

179 Para maiores informações sobre a Agesic e o modelo uruguaio de Governo Digital, consulte-se: BRUNET, Laura Nahabetián. **Del Gobierno Electrónico al Gobierno de la Información**. Montevideo: Amalio M. Fernández Editorial y Librería Jurídica, 2015.

Vide, ainda: NOUGRÈRES, Ana Brian. Uruguay y la Protección de Datos Personales. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coord.). **Direito & Internet IV**: Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019. p. 573. "La URCDP es una entidad autónoma de la Agencia uruguaya que tiene a su cargo el gobierno electrónico, que posee autonomía técnica. Está posicionada en el organigrama estatal y no está sujeta a mandatos o instrucción de poderes del estado."

do Uruguai"[180], conforme destacado em seu site oficial. Ou seja, tanto a URCDP quanto a ANPD são desprovidas de personalidade jurídica, estando ambas inseridas na Presidência da República.

Quanto a sua estrutura interna, a URCDP também apresenta equipe "enxuta", formada por um Conselho Executivo de 03 membros e um Conselho Consultivo de 05 membros, conforme organograma oficial:

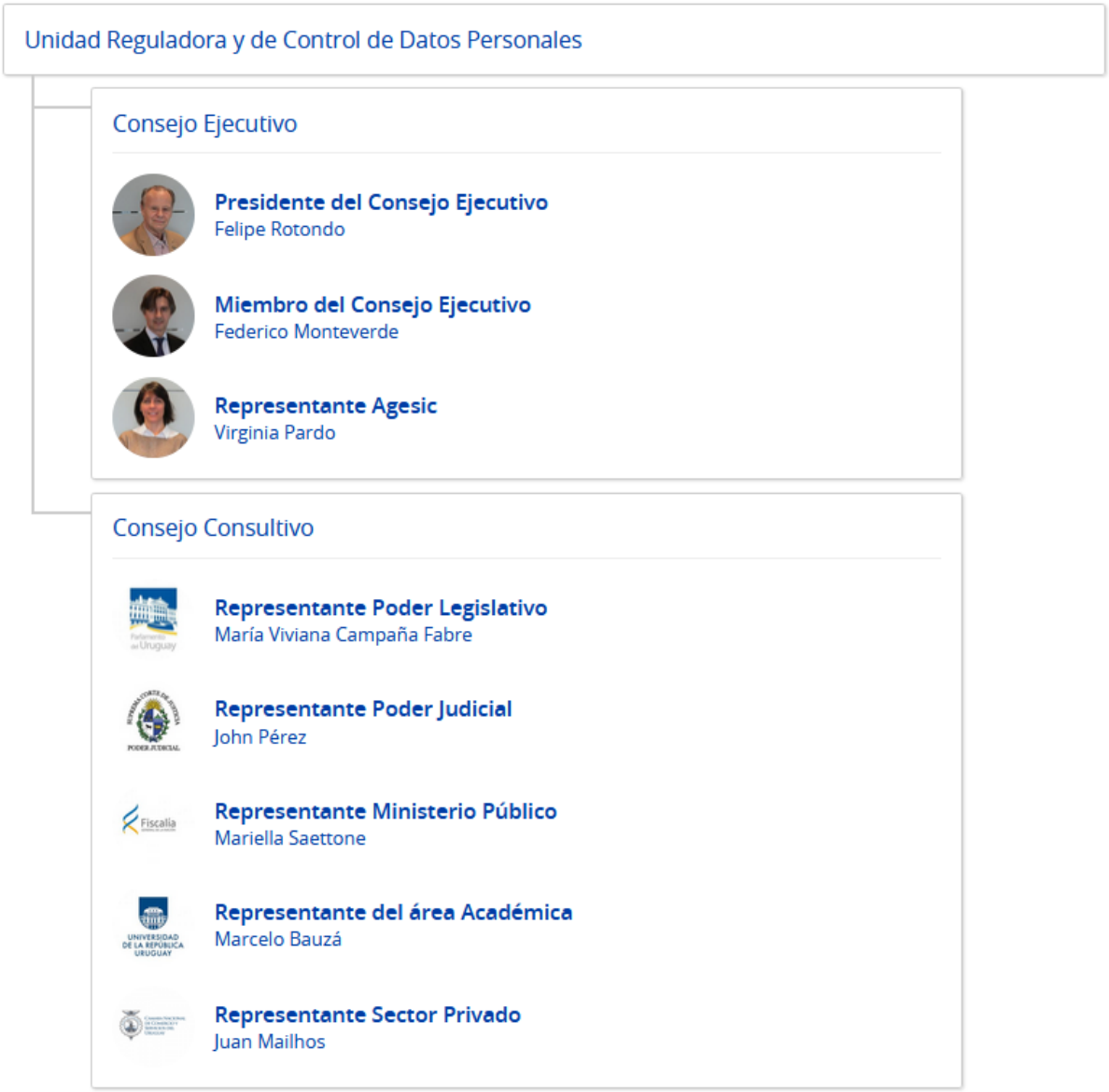


Figura 1. Organograma da URCDP. Disponível em <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/institucional/creacion-evolucion-historica>.

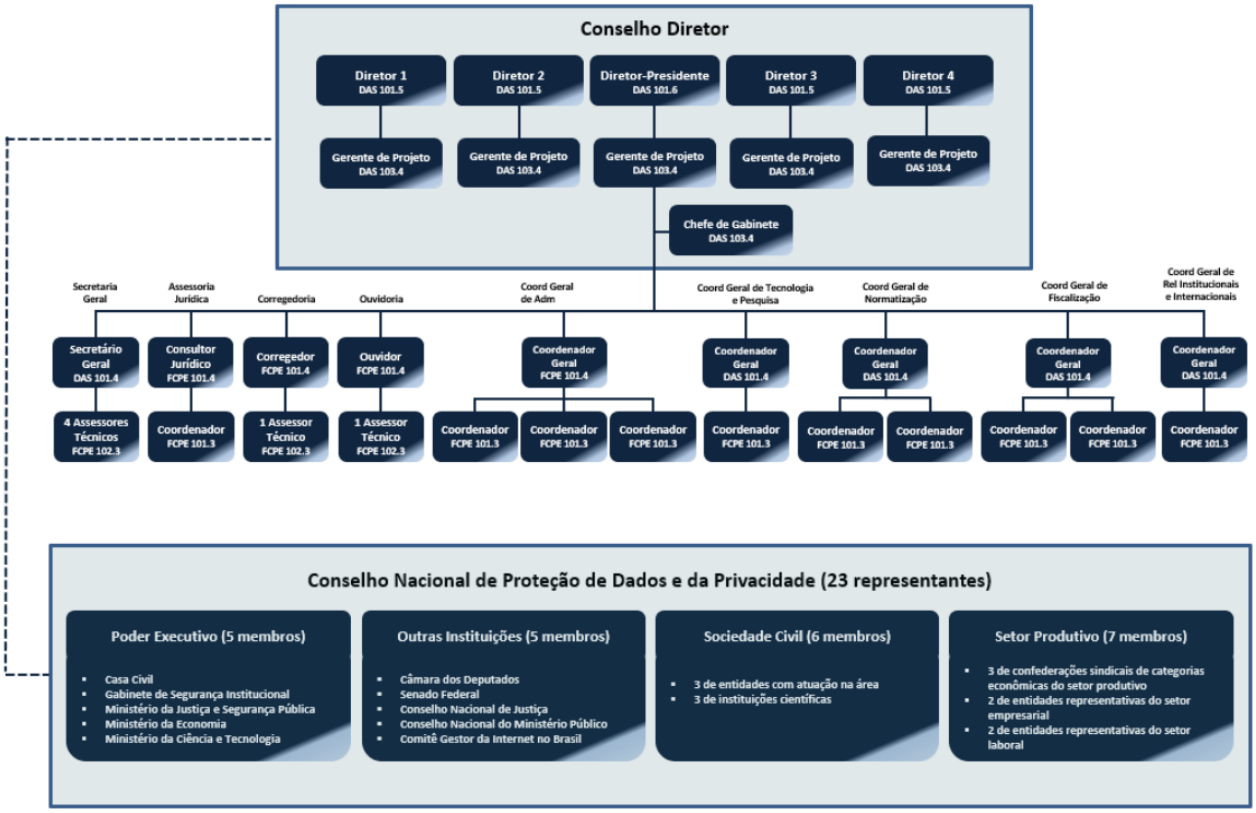
Neste ponto, inclusive, a ANPD estaria até mais bem estruturada, pois o seu Conselho Diretor (equivalente ao Conselho Executivo da URCDP) conta com 05 membros, ao passo que o órgão consultivo multissetorial brasileiro, o CNPD, conta com

[180] URUGUAY. **Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento – Agesic**. Disponível em <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/institucional/creacion-evolucion-historica>. Acesso em: 18 ago. 2021.

23 representantes titulares e suplentes. É, portanto, muito maior e mais representativo do que no modelo uruguaio.

Tanto na URCDP[181] quanto na ANPD[182] o mandato dos diretores tem duração de 04 anos, renovável por igual período. Merece destaque o fato de que a LGPD foi meticulosa quanto aos primeiros diretores, definindo, no art. 55-D, § 4º, regra especial que lhes atribuiu mandatos escalonados, com duração de 02, 03, 04, 05 e 06 anos, a fim de mitigar a possibilidade de nomeação da maioria do conselho pelos próximos Presidentes da República. Isto, em tese, tornaria os diretores menos propensos a pressões políticas, contribuindo para a independência da autoridade nacional. Esta regra especial aplica-se somente aos primeiros diretores. O mandato de seus sucessores terá duração comum de 04 anos, conforme art. 55-D, § 3º.

Com relação ao quadro de pessoal, a ANPD já dispõe de razoável número de profissionais e divisão interna de setores/atribuições, conquanto não chegue sequer próximo dos números apresentados por autoridades que são referência mundial nesse quesito[183]:



[181] NOUGRÈRES, Ana Brian. Uruguay y la Protección de Datos Personales. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coord.). **Direito & Internet IV**: Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019. p. 573. "La URCDP es dirigida por un Consejo que tiene tres miembros: el Director Ejecutivo de la agencia de gobierno electrónico uruguayo (o quien él designe delegándole sus funciones) y dos miembros designados por el Poder Ejecutivo por sus antecedentes personales, experiencia profesional y conocimientos de la materia, que se entiende garantiza su independencia de juicio, eficiencia, objetividad e imparcialidad para cumplir con sus obligaciones.

Estos tres miembros rotan anualmente para ocupar la presidencia de la URCDP. Con la excepción del Director Ejecutivo, duran cuatro años en sus cargos y pueden ser prorrogados sus mandatos."

[182] Vide LGPD, art. 55-D, § 3º.

[183] Referência mundial em termos de estrutura, a autoridade reguladora do Reino Unido, o Information Commissioner's Office – ICO, conta com mais de 500 profissionais: UNITED KINGDOM. **Information Commissioner's Office – ICO**. Disponível em <https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/>. Acesso em: 18 ago. 2021.

Figura 2. Organograma da ANPD. Disponível em <https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/estrutura-organizacional-1>.

Perceba-se que cada um dos 05 diretores da ANPD conta com um gerente de projetos dedicado, exclusivamente, a lhe assessorar, sendo que o Diretor-Presidente conta também com a chefia de gabinete. Além disso, fazem parte da estrutura da ANPD a secretaria-geral, assessoria jurídica, corregedoria, ouvidoria, coordenação de administração, coordenação de tecnologia e pesquisa, coordenação de normatização, coordenação de fiscalização e, finalmente, a coordenação de relações institucionais e internacionais. Postos esses ocupados por servidores investidos em cargo ou função de confiança, com dedicação exclusiva. Perceba-se, assim, que mesmo em seu estágio inicial a ANPD já está estruturada internamente de maneira satisfatória. O que não afasta a necessidade de reavaliação e aprimoramentos.

Com relação ao orçamento, o valor total disponibilizado para a Agesic, no ano de 2021, foi de 1.232.684.574,00 pesos uruguaios[184]. O que corresponde a aproximadamente 150 milhões de reais. Note-se que apenas uma fração desse valor será efetivamente destinada à URCDP, pois a Agesic custeia também o funcionamento de inúmeras outras estruturas administrativas. Por sua vez, a ANPD não teve orçamento oficial designado para o ano de 2021, uma vez que sua efetiva entrada em funcionamento, com a nomeação dos primeiros diretores, ocorreu ao final de 2020, quando a lei orçamentária para 2021 já havia sido aprovada. É, portanto, um ponto de atenção que deve merecer futuras análises.

Essa comparação estrutural entre URCDP e ANPD serve para demonstrar que, se as estruturas são semelhantes, é possível que ambas alcancem resultados parecidos. E caso isto se confirme – o que só o tempo dirá – certamente a ANPD terá desempenhado um excelente papel, a julgar pelo que a URCDP já produziu ao longo de pouco mais de uma década de funcionamento. Com efeito, em 2019 a autoridade uruguaia realizou ampla pesquisa no país para identificar qual era o grau de conhecimento da população local, a respeito de seus direitos em matéria de proteção de dados pessoais. E o resultado foi muito festejado. Cerca de 53% da população afirmou estar plenamente informada sobre seus direitos em matéria de proteção de dados pessoais[185]. Transpondo esse percentual para o Brasil, seria como se mais de 100 milhões de brasileiros afirmassem conhecer bem seus direitos previstos na LGPD. Algo que, certamente, ainda está muito distante da nossa realidade. Em 2020, foi realizada nova consulta e esse índice havia diminuído para 47%, o que continua sendo uma marca expressiva[186].

Outro importante marco para o Uruguai, e que certamente deve ser um dos objetivos buscados pelo Brasil, ao menos no médio prazo, é ser internacionalmente reconhecido por ter um "mercado de dados" adequado, que tanto respeite os direitos

---

[184] URUGUAY. **Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento – Agesic**. Disponível em <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/institucional/informacion-gestion/presupuesto/presupuesto-ano-2021>. Acesso em: 18 ago. 2021.

[185] URUGUAY. **Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento – Agesic**. Disponível em <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/nuevos-datos-resultados-5a-encuesta-conocimientos-actitudes-practicas>. Acesso em: 18 ago. 2021.

[186] URUGUAY. **Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento – Agesic**. Disponível em <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/datos-y-estadisticas/estadisticas/estudio-sobre-conocimientos-actitudes-practicas-ciudadania-digital-2020>. Acesso em: 18 ago. 2021.

do titular quanto permita o livre fluxo dos dados, o desenvolvimento econômico e a inovação. Pois bem, muito em virtude do trabalho da URCDP, o Uruguai já alcançou essa marca e, em agosto de 2012, recebeu a "decisão de adequação" da União Europeia, atestando que o referido país conta com uma autoridade reguladora independente[187]. Ou seja, desde 2012 o Uruguai já obteve reconhecimento marcante no plano internacional, mesmo apresentando uma autoridade reguladora com estrutura assaz diversa do preconizado na União Europeia.

Outra conquista do Uruguai, digna de nota, é ter sido o primeiro país não europeu a aderir à Convenção 108/1981 do Conselho da Europa[188], em agosto de 2013[189]. Adesão que se mantém até os dias atuais e foi ratificada em 07 de abril de 2021, por meio da Ley n. 19.948[190]. Finalmente, o Uruguai é o único Estado sul-americano integrante do Digital 9, grupo de 09 países que se auto intitulam "as nações mais avançadas do mundo em matéria digital" (the world's most advanced digital nations)[191]. Se o nosso vizinho sul-americano alcançou várias conquistas apresentando autoridade reguladora estruturada de modo semelhante à ANPD, por que duvidar que o Brasil também seja capaz de lograr isto?

Há ainda outras autoridades reguladoras de muito sucesso, cuja estrutura é diversa do modelo europeu. Por exemplo, no Canadá essa função é desempenhada pelo Office of the Privacy Commissioner[192], um órgão do Poder Legislativo dedicado especificamente à proteção de dados pessoais[193]. Apesar de não seguir "à risca" o modelo europeu, o Privacy Commissioner tem tradição na área e, inclusive, foi no

---

187 UNIÃO EUROPEIA. Comissão Europeia. **Decisão de Execução da Comissão**. Bruxelas: 21 ago. 2012. Disponível em <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32012D0484>. Acesso em: 30 jul. 2019. "Artigo 1º. Para efeitos do artigo 25º, n.º 2, da Diretiva 95/46/CE, considera-se que a República Oriental do Uruguai assegura um nível adequado de proteção dos dados pessoais transferidos a partir da União Europeia." Vide também o Considerando n. 10.

188 O Conselho da Europa é uma instituição internacional que promove os direitos humanos, incluindo a proteção de dados pessoais. Ele foi o responsável por criar a Convenção n. 108, em janeiro de 1981, tratado internacional aberto à adesão dos países interessados, sejam ou não europeus.

CONSELHO DA EUROPA. **Cooperação internacional**. Disponível em <https://edpb.europa.eu/international-cooperation_pt>. Acesso em: 20 ago. 2021.

Vide também: TENE, Omer. Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws. **Ohio State Law Journal**. Columbus: Moritz College of Law. v. 74, n. 06, p. 1217-1261, Nov. 2013. p. 1221.

189 CONSELHO DA EUROPA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. Strasbourg: 28 jan. 1981. Disponível em <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures>. Acesso em: 20 ago. 2021.

190 URUGUAY. Ley nº 19.948 – Protocolo de Enmienda del Convenio para la Protección de las Personas con Respecto al Tratamiento de Datos Personales. Disponível em <https://legislativo.parlamento.gub.uy/temporales/docu2658963172439.htm>. Acesso em: 22 ago. 2021.

191 DIGITAL 9. **About the D9**. Disponível em: <https://www.digital.govt.nz/digital-government/international-partnerships/the-digital-9/>. Acesso em: 20 jul. 2021.

192 CANADA. **Office of the Privacy Commissioner**. About the OPC. Disponível em <https://www.priv.gc.ca/en/about-the-opc/>. Acesso em: 20 ago. 2021.

193 LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional De Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020. p. 286-287. "O *Privacy Commissioner* canadense é definido como '*ombudsman*', que é um membro do Parlamento (*House of Commons* e Senado), cuja competência se restringe, exclusivamente, à proteção dos dados pessoais e privacidade (...).

No Canadá, pode-se entender o *Privacy Commissioner* como um ente que atua imparcialmente, devendo comunicar seus estudos e conclusões de forma transparente e dialogando com todos os *players*. Em outras palavras, este órgão não tem competência para decidir conflitos, nem tampouco resolver as reclamações individuais, porque não é um 'tribunal administrativo'."

Canadá que a expressão privacy by desing ganhou destaque, em 1995, a partir dos trabalhos de Ann Cavoukian[194].

Há outros exemplos que poderiam ser citados, mas que não serão mencionados em prol da brevidade deste texto. As linhas anteriores já são suficientes para demonstrar que a estrutura atual da ANPD, por si só, não é motivo para duvidar de sua independência e capacidade para exercer bem as funções que lhe foram atribuídas pela LGPD. Afinal, se outros países alcançaram bons resultados, valendo-se de autoridades reguladoras fora do modelo europeu, não há por que ser pessimista em relação à ANPD, que mal começou a operar.

3. POR QUE ACREDITAR NA ANPD? SÍNTESE DAS PRERROGATIVAS LEGAIS

A LGPD atribuiu à ANPD e a seus diretores uma série de garantias que, ao menos em um primeiro momento – e até que se possa reavaliar o modelo em vigor, à luz de casos concretos e de maior tempo de observação – parecem ser suficientes para conferir-lhe a necessária independência.

Com efeito, antes da confirmação dos diretores, os nomes indicados pelo Presidente da República devem se submeter a "sabatina" pelo Senado Federal, por força do art. 55-D, § 2º da LGPD. Ou seja, estão sujeitos ao mesmo tipo de controle aplicável aos ocupantes dos mais altos cargos da República, como por exemplo, os Ministros do Supremo Tribunal Federal. Maior rigor, inclusive, do que aquele aplicável aos Ministros de Estado, que são de livre escolha do Presidente. O mesmo artigo também exige que os indicados apresentem "reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade". Ainda que esses critérios contenham conceitos jurídicos indeterminados, podem servir de fundamento à negativa do Senado Federal, em casos extremos nos quais o indicado manifestamente não preencha os critérios.

Uma vez empossados, os diretores terão mandato por prazo fixo (LGPD art. 55-D, § 3º). Durante esse período, não se sujeitam a afastamento preventivo, salvo por decisão fundamentada do próprio Presidente da República, após recomendação de comissão especial, conforme art. 55-E, § 2º. Por sua vez, o afastamento definitivo do cargo somente poderá decorrer de "renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar", instaurado pelo "Ministro de Estado Chefe da Casa Civil da Presidência da República" (art. 55-E). Novamente, são garantias mais amplas do que as deferidas aos Ministros de Estado.

Durante o exercício de suas funções, o art. 55-B da LGPD assegura "autonomia técnica e decisória à ANPD" e, muito mais do que simples retórica, tal dispositivo acarreta importante repercussão prática. Caso ele não existisse, haveria a possibilidade de decisões tomadas pelo Conselho Diretor da ANPD serem submetidas a reexame de instâncias superiores do Poder Executivo, eventualmente até do próprio Presidente da República, por força do art. 56, § 1º da Lei nº 9.784/1999 (Lei Geral do Processo Administrativo). O que certamente acrescentaria um perigoso componente político a tais decisões. Contudo, a mencionada redação do art. 55-B da LGPD afasta essa possibilidade, assegurando que as decisões do Conselho Diretor da ANPD sejam

[194] CANADA. Ontario. **Privacy-enhancing technologies**: the path to anonymity. v. I. 1995.

definitivas na esfera administrativa[195]. Aspecto reiterado no art. 73, parágrafo único, do regimento interno da autoridade[196]. Neste ponto, eventual conversão da ANPD em agência reguladora, estruturada como autarquia, encerraria a discussão uma vez que o art. 3º da Lei n. 13.848/2019 (Lei das Agências Reguladoras) expressamente afasta a subordinação hierárquica.

Prosseguindo, mesmo após o término do mandato e efetiva desvinculação da ANPD, os ex-diretores permanecem sujeitos à fiscalização do Poder Público e da sociedade. Isto porque o art. 55-F da LGPD lhes impõe prazo de desincompatibilização de 06 meses. Referido prazo é coloquialmente chamado de "quarentena", mesmo antes da pandemia de Covid-19. Durante esse período, os ex-diretores não poderão se envolver em qualquer atividade potencialmente causadora de conflito de interesses, em virtude das informações a que tiveram acesso enquanto integravam a ANPD, nos termos da Lei n. 12.813/2013 (Lei do Conflito de Interesses).

Nota-se, então, que a LGPD cuidou de estabelecer uma série de prerrogativas e cautelas aplicáveis em todas as fases do processo, com o objetivo de assegurar que as decisões da ANPD sejam técnicas e independentes. Vistas essas prerrogativas, cumpre agora realizar uma sucinta análise das primeiras medidas adotas pela ANPD.

4. ANÁLISE DAS PRIMEIRAS MEDIDAS ADOTADAS PELA ANPD

A ANPD entrou efetivamente em funcionamento no dia 06 de novembro de 2020, quando foram empossados os seus primeiros diretores[197]. Nas linhas seguintes, optou-se por analisar algumas medidas oficiais[198] por ela adotadas dessa data até abril de 2021, mesmo recorte temporal feito pela própria autoridade, ao publicar a seguinte "linha do tempo":

[195] PFEIFFER, Roberto Augusto Castellanos. A Saga da Autoridade Nacional de Proteção de Dados: Do veto à Lei nº 13.853/2019. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coord.). **Direito & Internet IV**: Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019. p. 458. "(...) entendo que o fato da autonomia decisória ter sido expressamente estatuída pelo art., 55-B na redação conferida pela Lei nº 13.853/2019, afasta a interpretação de ser possível a interposição de recursos contra decisões da ANPD dirigidos ao Presidente da República."

[196] BRASIL. Autoridade Nacional de Proteção de Dados. **Regimento Interno**: Portaria ANPD n. 01/2021. Disponível em <https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618>. Acesso em: 17 ago. 2021.

[197] Consulte-se o histórico detalhado no primeiro tópico deste texto.

[198] Evidentemente, houve uma série de medidas extraoficiais, como reuniões de alinhamento entre os diretores, entrevistas com os servidores que viriam a constituir a equipe de apoio, formalidades burocráticas para a criação de sua sede física e inclusão do site no domínio ".gov.br", etc. Ainda que sejam importantes, estas medidas não serão aqui analisadas, priorizando-se apenas o exame de alguns documentos oficiais da ANPD arrolados no texto.

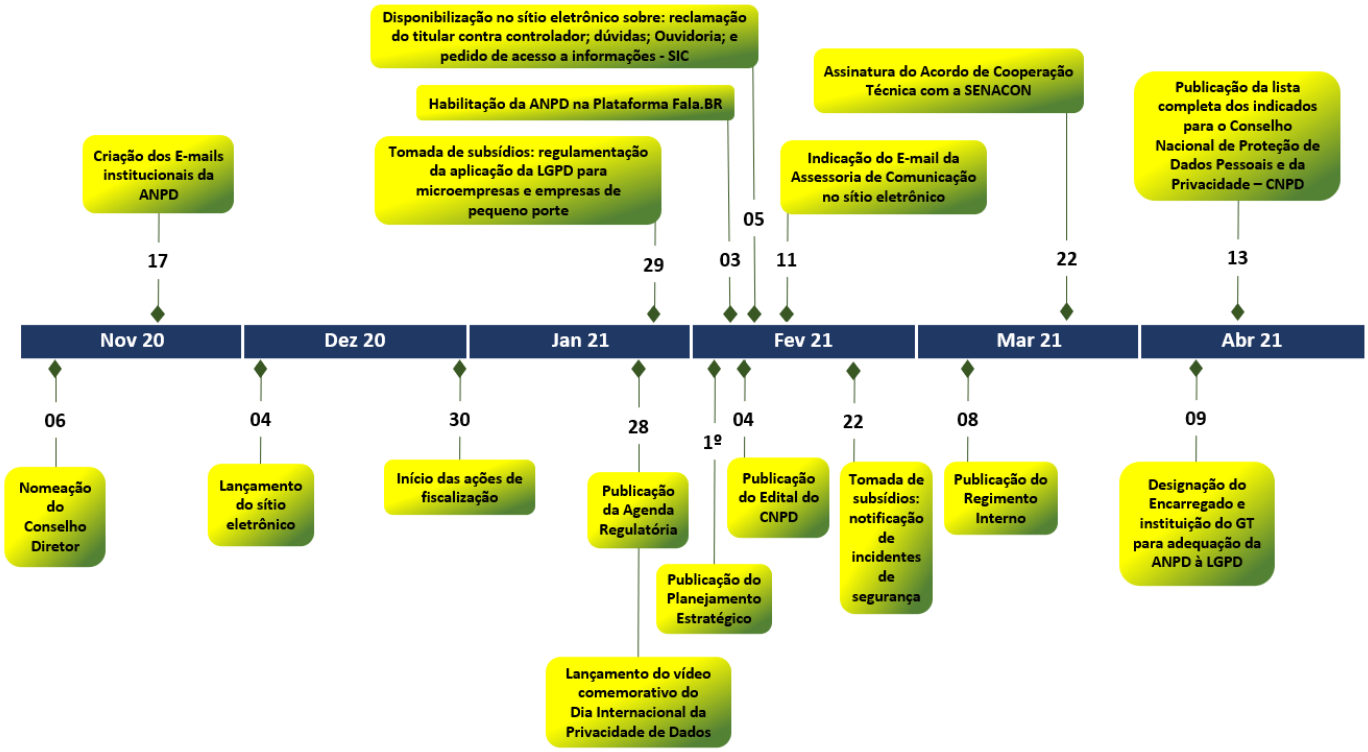


Figura 3. Linha do Tempo na ANPD. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/noticias/confira-linha-do-tempo-com-as-principais-acoes-da-anpd>.

Este artigo optou por focar em 03 medidas tomadas pela ANPD, tendo em vista o limite máximo de laudas fixado para o texto: 1) agenda regulatória para o biênio 2020-2021; 2) regimento interno; e 3) nota técnica sobre a política de privacidade do WhatsApp.

Em 27 de janeiro de 2021, a ANPD elaborou sua agenda regulatória para o biênio 2021-2022[199], dando a conhecer qual a estratégia para esse período, elencando os temas a serem tratados e a data estimada para a conclusão de cada um deles. A publicação dessa agenda não é imposta pela LGPD, tendo sido feita espontaneamente pela ANPD como forma de sinalizar seus próximos passos ao mercado e engajar possíveis interessados, além de demonstrar o compromisso do órgão regulador com a transparência. A agenda divide-se em 3 fases. A primeira compreende as medidas necessárias para o bom funcionamento da autoridade, que devem ocorrer até o final de 2021, tais como a confecção do regimento interno e do planejamento estratégico, além dos atos normativos que embasarão a gradação de sanções e o procedimento para sua aplicação, nos termos dos artigos 52 e 53 da LGPD. Bem como a produção de atos normativos regulando o tratamento diferenciado a microempresas e empresas de pequeno porte, o procedimento para a comunicação de incidentes de segurança e maior detalhamento das regras sobre elaboração dos relatórios de impacto à proteção de dados pessoais.

O regimento interno da ANPD já foi publicado e será analisado a seguir. O formulário para comunicação de incidentes de segurança também já está disponível

[199] BRASIL. Autoridade Nacional de Proteção de Dados. **Agenda Regulatória para o biênio 2021-2022**: Portaria ANPD n. 11/2021. Disponível em <https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>. Acesso em: 17 ago. 2021.

no site da autoridade[200]. Por sua vez, as resoluções sobre pequenas empresas e relatório de impacto foram objeto de consulta pública, mas os normativos correspondentes não haviam sido publicados até a conclusão deste texto. As fases 2 e 3 da agenda regulatória, previstas para ocorrer em 2022, igualmente compreendem tópicos importantes, como o detalhamento das atribuições do encarregado pelo tratamento de dados pessoais, diretrizes para a transferência internacional de dados, direitos do titular dos dados e guia sobre a utilização das bases legais (hipóteses de tratamento). Em suma, a agenda regulatória demonstra o compromisso da autoridade nacional com a transparência e, na visão deste autor, foi feliz na escolha dos temas prioritários.

Prosseguindo ao segundo ponto objeto de exame, o regimento interno da ANPD201 foi concluído em 08 de março de 2021. Ele adota técnicas modernas de gestão de processos e tomada de decisão, com destaque para os "circuitos deliberativos" (art. 40 e seguintes), procedimento por meio do qual cada diretor deposita eletronicamente o seu voto, sem a necessidade de reunião síncrona, presencial, para decidir. Algo semelhante ao que já ocorria no plenário virtual do STF[202]. Votos proferidos por diretores que venham a se afastar temporariamente ou que tenham se desligado da ANPD serão normalmente computados, para todos os fins (art. 19, § 1º do regimento interno), o que tende a imprimir celeridade às decisões do órgão. Outra medida importantíssima para a racionalização do processo decisório é a possibilidade de julgar simultaneamente, com um mesmo voto, reclamações de titulares de dados pessoais que digam respeito a tema semelhante, de maneira que uma decisão possa solucionar dezenas ou quiçá milhares de casos (art. 2º, § 6º do Decreto n. 10.474/2020). Semelhante aos mecanismos de resolução de demandas repetitivas do processo civil. Estes são apenas alguns pontos do regimento interno da ANPD, dignos de nota.

No âmbito das atividades de fiscalização, a primeira medida concreta tomada pela ANPD teve por objeto a polêmica modificação da política de privacidade do aplicativo de mensagens instantâneas WhatsApp, visando ao compartilhamento de dados pessoais com o Facebook e com terceiros. A ANPD fiscalizou esse documento e sobre ele emitiu nota técnica[203] trazendo importantes considerações. Em 04 de janeiro de 2021, o WhatsApp notificou seus usuários informando que passaria a compartilhar com o Facebook dados pessoais contidos nas mensagens de WhatsApp, sobretudo na versão empresarial deste aplicativo (WhatsApp Business). Isso provocou indignação nos usuários e grande repercussão na imprensa[204]. Em seguida, a ANPD solicitou informações das empresas envolvidas, analisou a nova política de privacidade e sobre

---

[200] BRASIL. Autoridade Nacional de Proteção de Dados. **Incidentes de segurança com dados pessoais e sua avaliação para fins de comunicação à ANPD**. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>. Acesso em: 22 ago. 2021.

[201] BRASIL. Autoridade Nacional de Proteção de Dados. **Regimento Interno**: Portaria ANPD n. 01/2021. Disponível em <https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618>. Acesso em: 17 ago. 2021.

[202] Não é o escopo deste texto aprofundar a análise a respeito dos prós e contras desse modelo.

[203] BRASIL. Autoridade Nacional de Proteção de Dados. **Nota Técnica ANPD n. 02/2021**. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NOTATECNICADACGTP.pdf>. Acesso em: 22 ago. 2021.

[204] SCHREIBER, Mariana. **Após reação negativa, WhatsApp adia para maio 'ultimato' para usuário compartilhar dados com Facebook**. Brasília: 15 jan. 2021. Disponível em: <https://www.bbc.com/portuguese/brasil-55680262>. Acesso em: 22 ago. 2021.

ela emitiu recomendação técnica, cujos principais pontos serão criticamente analisados a seguir. Primeiramente, a autoridade nacional enquadrou o Facebook e demais empresas que tenham acesso aos dados do WhatsApp como controladoras (itens 95 e 96 da Nota Técnica). Não enfrentou, porém, a polêmica[205] de definir se, mesmo na omissão da LGPD, o Brasil adota ou não a figura do controle conjunto (joint controllership)[206]. A ANPD foi enfática ao exigir que a política de privacidade do WhatsApp informe com clareza quis são as principais bases legais utilizadas (itens 82, 104 a 107 e 135 da Nota Técnica), tal como já era feito na versão europeia do mesmo documento. Aqui, na visão deste autor, a ANPD cometeu um erro técnico. Com efeito, há substancial diferença entre as previsões legislativas da Europa (GDPR) e do Brasil (LGPD) acerca da publicidade das bases legais:

> GDPR. Art. 13. 1. Quando os dados pessoais forem recolhidos junto do titular, o responsável pelo tratamento faculta-lhe, quando da recolha desses dados pessoais, as seguintes informações:
> (...)
> c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;

> LGPD. Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;

---

[205] Contra a existência de controle conjunto no Brasil: LEONARDI ADVOGADOS. **Publicidade Personalizada e LGPD**. Parecer s/n, de 26.07.2021. Autor(a): Marcel Leonardi. p. 15. "(...) a LGPD não criou a figura do 'co-controlador', ou 'controlador conjunto' ('*joint controller*'), prevista no artigo 26 (1, 2 e 3) do GDPR, pela qual são considerados co-controladores os agentes de tratamento que determinam conjuntamente as finalidades e os meios de tratamento, com responsabilidade conjunta, inclusive em relação ao atendimento dos direitos dos titulares. (...) Assim sendo, no contexto brasileiro, ainda que situações conjuntas de tratamento ocorram na prática com relativa frequência, a LGPD em tese considera cada empresa uma controladora independente."

A favor da existência de controle conjunto: PARENTONI, Leonardo. Compartilhamento de Dados Pessoais e a Figura do Controlador. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Coord.). **Compliance de dados à luz da LGPD**. No prelo. "Avançando um pouco mais, existem legislações que abordam as diferentes espécies de controlador e de operador. A LGPD, porém, não tratou do tema. O que não significa que tais espécies inexistam no Brasil. Pelo contrário, elas decorrem do próprio funcionamento do mercado, do modo como os tratamentos de dados são executados na prática, visto que os agentes de tratamento estão continuamente inovando e buscando novos modelos de negócio."

[206] UNIÃO EUROPEIA. European Data Protection Board. **Guideline nº 07/2020: on the concepts of controller and processor in the GDPR**. Bruxelas: 02 Set. 2020. Disponível em: <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_pt>. Acesso em: 14 fev. 2021. p. 03. "The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. Joint participation can take the form of a common decision taken by two or more entities or result from converging decisions by two or more entities, where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing."

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Perceba-se que a LGPD, diferentemente do que fez o GDPR, não exigiu a publicação das bases legais na política de privacidade. Isso é inequívoco e decorre da própria comparação entre os dispositivos citados, já que o art. 9º não incluiu as bases legais na lista dos itens que devem ser publicados. O que poderá ser feito é incluir essa exigência via futura regulamentação da ANPD sobre o tema, a qual está prevista para ocorrer na fase 3 da agenda regulatória, a partir do segundo semestre de 2022.

A ANPD, portanto, recomendou ao WhatsApp (item 82 da Nota Técnica) que incluísse em sua política de privacidade um tópico que não consta da lei nem da própria regulamentação da autoridade. Sendo que o item 104 da Nota Técnica complementou dizendo que não se vislumbram "razões jurídicas que justifiquem a sua omissão no Brasil". Ora, a razão jurídica é a própria inexistência de dispositivo legal ou resolução administrativa exigindo a publicação de bases legais, conforme art. 5º, II da Constituição de 1988 (princípio da legalidade) e art. 3º, V da Lei n. 13.874/2019 (Declaração de Direitos de Liberdade Econômica). Assim, o autor considera que a ANPD se equivocou neste ponto, ao tratar o tema como "recomendação" (ou seja, algo vinculante, impositivo), ao invés de simples sugestão (facultativa, cujo não atendimento não sujeita o destinatário a qualquer sanção e não precisa ser sequer justificado). Não se desconhece que publicar as bases legais é uma boa prática internacionalmente aceita e que depõe a favor do controlador, em termos de transparência e accountability, devendo ser estimulada. Coisa diversa, porém, é recomendá-la (no sentido de imposição do órgão regulador) sem o devido substrato normativo prévio.

Outro ponto importante da nota técnica foi destacar (nos itens 113 a 118) que o Brasil deverá utilizar o critério da estrita necessidade do tratamento de dados pessoais no contexto de um contrato, para diferenciar as hipóteses de cabimento da base legal do contrato e do legítimo interesse, à semelhança do que já ocorre no modelo europeu e no Reino Unido[207]. Isto significa que somente atividades de tratamento estritamente necessárias para a execução do contrato ou de procedimentos preliminares a ele se incluem na referida base legal. Por conseguinte, atividades de mero aprimoramento do modelo de negócios do controlador devem se basear no legítimo interesse, com todas as consequências advindas disto, por exemplo, a obrigatoriedade[208] de se elaborar previamente um relatório (legitimate interest assessment).

---

[207] UNITED KINGDOM. **Information Commissioner's Office – ICO**. Disponível em <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/>. Acesso em: 18 ago. 2021. p. 01. "The processing must be necessary. If you could reasonably do what they want by processing less data, or using their data in a less intrusive way, this basis will not apply."

[208] LEONARDI, Marcel. Principais Bases Legais de Tratamento de Dados Pessoais no Setor Privado. *In*: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla et al. (Coord.). **Caderno Especial – Lei Geral de Proteção de Dados**. São Paulo: Revista dos Tribunais, 2019. p. 80. "(...) entendemos que o artigo 10, § 3º, estipula que sempre deve ser elaborado relatório de impacto à proteção de dados pessoais no caso de tratamento de dados pessoais baseado em legítimo interesse, pois esse documento pode ser exigido pela Autoridade a qualquer tempo, não podendo ser elaborado apenas quando de sua requisição. Já nos casos do artigo 38,

Ainda no que toca às bases legais, a autoridade nacional deixou transparecer (item 113 da Nota Técnica) que a utilização de qualquer delas decorre da finalidade[209] do tratamento dos dados, não sendo cabível a cumulação discricionária de bases legais[210], assim considerada a situação na qual o controlador arrola uma série de bases legais (muitas vezes contraditórias) como fundamento para a mesma operação de tratamento de dados pessoais, afirmando que preferencialmente utiliza a base "x", mas que também utiliza, subsidiariamente, as bases "y" e "z", para se resguardar, caso o entendimento da autoridade reguladora seja pelo não cabimento de "x". Esse tipo de cumulação de pedidos tem lugar no processo civil, mas não na sistemática da LGPD. Nesta lei, cada hipótese de tratamento apresenta alcance subjetivo e objetivo próprios, sendo que algumas demandam ainda a confecção de documentos extras, como é o caso do legítimo interesse. Portanto, é ônus do controlador conhecer as suas operações de tratamento de dados pessoais e associá-las à base legal correta, conforme o contexto e a finalidade do tratamento.

Igualmente digno de nota foi o fato de que, pela primeira vez, a ANPD esboçou uma lista dos pontos que devem constar de um relatório de impacto à proteção de dados pessoais (item 98 da Nota Técnica), providência presente na fase 1 da agenda regulatória e prevista para ser deliberada no primeiro semestre de 2021, mas cuja resolução ainda não havia sido publicada até data de conclusão deste artigo. Portanto, foi salutar que a ANPD informasse aos agentes de tratamento, antecipadamente (e aqui de forma correta, sem caráter vinculativo) quais tópicos deverão constar do mencionado relatório.

Inúmeros outros pontos da nota técnica são interessantes e poderiam ser abordados. Porém, em prol da objetividade deste texto, optou-se por focar nos itens acima. Em síntese, a ANPD sinalizou a WhatsApp e Facebook, dois gigantes do mercado, que será firme na defesa do sistema brasileiro de proteção de dados pessoais e de seus usuários. Um claro recado de que o Brasil precisa ser respeitado. Recado que, aparentemente, foi bem compreendido, pois as referidas empresas seguiram espontaneamente as recomendações da autoridade nacional.

5. CONCLUSÃO

Logo que a ANPD foi criada, não faltaram críticas e manifestações de pessimismo, vociferando que ela não teria a independência necessária para bem executar suas funções, por ter sido estruturada como órgão público, diverso do que preconiza o modelo europeu. Este texto então analisou o formato de algumas autoridades internacionais de proteção de dados, demonstrando que a estrutura inicial da ANPD, por si só, não é empecilho a que ela alcance bons resultados, pois outros países – com destaque para o Uruguai – lograram importantes conquistas, inclusive no plano

a Autoridade pode determinar a elaboração do relatório em situações específicas, ainda pendentes de regulamentação."

[209] RODOTÀ, Stefano. **Elaboratori Elettronici e Controllo Sociale**. Bologna: Il Mulino, 1973. p. 32-33. "(...) non deve essere confuso il profilo della legittimità della raccolta di informazioni per un fine determinato con quello, diverso, di una disciplina tendente a garantire la conformità dell'uso al fine."

[210] PARENTONI, Leonardo. Compartilhamento de Dados Pessoais e a Figura do Controlador. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Coord.). **Compliance de dados à luz da LGPD**. No prelo. "*Não* se trata de escolha discricionária do controlador, pois a definição de bases legais é ato vinculado: a finalidade do tratamento é que define qual a base cabível. Mas há situações nas quais a mesma operação de tratamento, com a mesma finalidade, pode se amoldar a mais de uma base legal."

internacional, valendo-se de uma autoridade estruturada de modo semelhante à ANPD. Além disso, a recente transformação da ANPD em autarquia especial, feita pela Medida Provisória n. 1.124/2022, tende a superar, ao menos em tese, a maior parte dos óbices levantados contra a autoridade reguladora brasileira.

Para além dessa análise estrutural, o texto também examinou as primeiras medidas concretas adotadas pela autoridade brasileira, o que corroborou a opinião de que ela merece um voto de confiança, já que estas medidas foram altamente positivas. Com efeito, em poucos meses a ANPD se estruturou satisfatoriamente, publicou uma agenda regulatória e vem cumprindo-a, trazendo importantes sinalizações aos agentes de tratamento e aos titulares de dados pessoais, especialmente com relação a pontos nos quais a LGPD é dúbia ou omissa, deliberadamente delegando à autoridade nacional a definição de padrões e o preenchimento de lacunas.

Isto não significa que o autor concorde com todas as medidas tomadas pela ANPD até aqui. Com efeito, algumas delas são tecnicamente discutíveis e foram questionadas no texto. Por exemplo, quanto à obrigatoriedade de se publicar as bases legais na política de privacidade, pois inexiste no país, ao menos até agora, lei ou ato infralegal impondo essa publicação. Apesar disso, o saldo das medidas analisadas é deveras positivo para a própria autoridade nacional, para os agentes de tratamento de dados pessoais e, principalmente, para a sociedade brasileira. Algumas críticas e divergências técnicas são naturais e esperadas. Elas certamente ocorreriam também em relação a qualquer outra autoridade reguladora, inclusive aquelas já constituídas e estabilizadas há décadas. O objetivo é contribuir com o aprimoramento do sistema, e não desacreditar a ANPD.

Finalmente, na visão deste autor o principal papel de uma autoridade de proteção de dados, em qualquer país, é fomentar a cultura nacional de proteção de dados[211], conscientizando todos os participantes do ecossistema local a respeito de seus direitos e deveres, do que efetivamente se espera de cada um deles. No Brasil, como a LGPD é recente e a autoridade nacional mal começou a operar, tal prioridade ganha ainda mais relevo. O momento, portanto, é de conscientização e definição das "regras do jogo", não de fiscalização e punição. Afinal, para bem cumprir as regras, é preciso que antes elas sejam claramente definidas e compreendidas. Nesse sentido, as primeiras medidas da ANPD foram na direção correta.

[211] Assim como cada país tem cultura e tradição histórica própria, cada um deles apresenta peculiaridades em sua política de proteção de dados pessoais. Ainda que haja semelhanças e mecanismos de harmonização internacional, dois países nunca são iguais. Sobre esse tema, vide, por exemplo: WHITMAN, James Q. The Two Western Cultures of Privacy: Dignity versus Liberty. **Yale Law Journal**. Yale: The Yale Law Journal. v. 113, n. 06, p. 1151-1221, Apr. 2004. p. 1159-1163.

6. REFERÊNCIAS

BOBBIO, Norberto. Da Estrutura à Função: Novos Estudos de Teoria do Direito. Tradução: Daniela Beccaccia Versiani. Barueri: Manole, 2007.

BRASIL. Agência Brasil. Desemprego registrou taxa média de 13,5% em 2020. Brasília: 10 mar. 2021. Disponível em https://agenciabrasil.ebc.com.br/economia/noticia/2021-03/desemprego-registrou-taxa-media-de-135-em-2020 Acesso em: 17 ago. 2021.

BRASIL. Autoridade Nacional de Proteção de Dados. Agenda Regulatória para o biênio 2021-2022: Portaria ANPD n. 11/2021. Disponível em https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313 Acesso em: 17 ago. 2021.

_____. Autoridade Nacional de Proteção de Dados. Incidentes de segurança com dados pessoais e sua avaliação para fins de comunicação à ANPD. Disponível em https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca Acesso em: 22 ago. 2021.

_____. Autoridade Nacional de Proteção de Dados. Nota Técnica ANPD n. 02/2021. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NOTATECNICADACGTP.pdf Acesso em: 22 ago. 2021.

_____. Autoridade Nacional de Proteção de Dados. Regimento Interno: Portaria ANPD n. 01/2021. Disponível em https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618 Acesso em: 17 ago. 2021.

_____. Autoridade Nacional de Proteção de Dados. Presidente da República designa membros do CNPD. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/presidente-da-republica-designa-membros-do-cnpd Acesso em: 17 ago. 2021.

_____. Presidência da República. Mensagem de Veto n. 451/2018. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm Acesso em: 17 ago. 2021.

_____. Câmara dos Deputados. Projeto de Lei nº 4.060/2012. Disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066 Acesso em: 17 ago. 2021.

_____. Câmara dos Deputados. Projeto de Lei nº 5.276/2016. Disponível em http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 Acesso em: 17 ago. 2021.

BRUNET, Laura Nahabetián. Del Gobierno Electrónico al Gobierno de la Información. Montevideo: Amalio M. Fernández Editorial y Librería Jurídica, 2015.

CANADA. Office of the Privacy Commissioner. About the OPC. Disponível em https://www.priv.gc.ca/en/about-the-opc/ Acesso em: 20 ago. 2021.

CANADA. Ontario. Privacy-enhancing technologies: the path to anonymity. v. I. 1995.

CONSELHO DA EUROPA. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Disponível em https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures Acesso em: 17 ago. 2021.

_____. Cooperação internacional. Disponível em https://edpb.europa.eu/international-cooperation_pt Acesso em: 20 ago. 2021.

DIGITAL 9. About the D9. Disponível em: https://www.digital.govt.nz/digital-government/international-partnerships/the-digital-9/ Acesso em: 20 jul. 2021.

DONEDA, Danilo Cesar Maganhoto. Da privacidade à proteção e dados pessoais. Rio de Janeiro: Renovar, 2006.

_____. Rumo à Autoridade Nacional de Proteção de Dados. In: DE LUCCA, Newton; **SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL**, Renata Mota (Coord.). Direito & Internet IV: Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019.

EUROPEAN COMMISSION. What are Data Protection Authorities (DPAs)? Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en Acesso em: 17 ago. 2021.

GREENLEAF, Graham. Global data privacy 2021: DPAs joining networks are the rule. Privacy Laws & Business International Report. London: Privacy Laws & Business. v. 170, n. 01, p. 23-26, Jan. 2021. p. 23. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3874834 Acesso em: 24 ago. 2021.

ISRAEL. Privacy Protection Authority. About PPA. Disponível em https://www.gov.il/en/departments/about/about_ppa Acesso em: 20 ago. 2021.

JOTA. Ex-Ministro diz que não há vício de inconstitucionalidade na criação da ANPD. São Paulo: 31 jul. 2018. Disponível em https://www.jota.info/docs/ex-ministro-diz-que-nao-ha-vicio-de-inconstitucionalidade-na-criacao-da-anpd-31072018 Acesso em: 17 ago. 2021.

KOPP, Christel; LODGE, Martin. What is regulation? An interdisciplinary concept analysis. Regulation & Governance. Hoboken: Wiley. v. 11, n. 01, p. 01-43, Jul. 2015; e BALDWIN, Robert; CAVE, Martin; LODGE, Martin. Understanding Regulation: Theory, Strategy, and Practice. Oxford: Oxford University Press, 2012.

KORFF, Douwe; GEORGES, Marie. The DPO Handbook: Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation. Rome: T4Data Programme, 2019. Available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9127859 Access: 05 Jul. 2020.

LEONARDI ADVOGADOS. Publicidade Personalizada e LGPD. Parecer s/n, de 26.07.2021. Autor(a): Marcel Leonardi.

LEONARDI, Marcel. Principais Bases Legais de Tratamento de Dados Pessoais no Setor Privado. In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla et al. (Coord.). Caderno Especial – Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2019.

LIMA, Cíntia Rosa Pereira de. Autoridade Nacional De Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados. São Paulo: Almedina, 2020.

_____; **PEROLI, Kelvin**. Desafios para a Atuação Independente da Autoridade Nacional de Proteção de Dados Pessoais Brasileira à Luz das Exigências Internacionais para a Adequada Proteção de Dados Pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coord.). Direito & Internet IV: Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019.

LYNSKEY, Orla. The Foundations of EU Data Protection Law. Oxford: Oxford University Press, 2015.

NOUGRÈRES, Ana Brian. Uruguay y la Protección de Datos Personales. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coord.). Direito & Internet IV: Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019.

PARENTONI, Leonardo. Autoridade Nacional de Proteção de Dados Brasileira: Uma visão otimista. Revista do Advogado. São Paulo: AASP, Ano XXXIX, n. 144, p. 209-219, nov. 2019.

_____. Compartilhamento de Dados Pessoais e a Figura do Controlador. In: **FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Coord.)**. Compliance de dados à luz da LGPD. No prelo.

PFEIFFER, Roberto Augusto Castellanos. A Saga da Autoridade Nacional de Proteção de Dados: Do veto à Lei nº 13.853/2019. In: DE LUCCA, Newton; SIMÃO FILHO, **Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coord.).** Direito & Internet IV: Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019.

RODOTÀ, Stefano. Elaboratori Elettronici e Controllo Sociale. Bologna: Il Mulino, 1973.

SARMENTO E CASTRO, Catarina. Direito da Informática, Privacidade e Dados Pessoais. Coimbra: Almedina, 2005.

SCHREIBER, Mariana. Após reação negativa, WhatsApp adia para maio 'ultimato' para usuário compartilhar dados com Facebook. Brasília: 15 jan. 2021. Disponível em: https://www.bbc.com/portuguese/brasil-55680262 Acesso em: 22 ago. 2021.

SILVA, Victor Hugo. Autoridade Nacional de Proteção de Dados é criada por Medida Provisória. São Paulo: 28 dez. 2018. Disponível em: https://tecnoblog.net/273018/mp-autoridade-nacional-protecao-dados/ Acesso em: 17 ago. 2021.

TENE, Omer. Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws. Ohio State Law Journal. Columbus: Moritz College of Law. v. 74, n. 06, p. 1217-1261, Nov. 2013.

TIKKINEN-PIRI, Christina; ROHUNEN, Anna; MARKKULA, Jouni. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review. Amsterdam: Elsevier. v. 34, n. 01, p. 134-153, Feb. 2018.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT Acesso em: 17 ago. 2021.

_____. Comissão Europeia. Decisão de Execução da Comissão. Bruxelas: 31 jan. 2011. Disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AL%3A2011%3A027%3A0039%3A0042%3Aen%3APDF Acesso em: 22 ago. 2021.

_____. Comissão Europeia. Decisão de Execução da Comissão. Bruxelas: 21 ago. 2012. Disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32012D0484 Acesso em: 30 jul. 2019.

_____. European Data Protection Board. Guideline nº 07/2020: on the concepts of controller and processor in the GDPR. Bruxelas: 02 Set. 2020. Disponível em: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_pt Acesso em: 14 fev. 2021.

_____. Tratado sobre o Funcionamento da União Europeia. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012E/TXT Acesso em: 17 ago. 2021.

UNITED KINGDOM. Information Commissioner's Office – ICO. Disponível em https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/ Acesso em: 18 ago. 2021.

UNITED STATES OF AMERICA. Federal Trade Commission – About the FTC. Disponível em: https://www.ftc.gov/about-ftc Acesso em: 17 ago. 2021.

_____. Federal Trade Commission – News & Events. Disponível em: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions Acesso em: 17 ago. 2021.

URUGUAY. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento – Agesic. Disponível em https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/institucional/creacion-evolucion-historica Acesso em: 18 ago. 2021.

_____. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento – Agesic. Disponível em https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/institucional/informacion-gestion/presupuesto/presupuesto-ano-2021 Acesso em: 18 ago. 2021.

_____. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento – Agesic. Disponível em https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/nuevos-datos-resultados-5a-encuesta-conocimientos-actitudes-practicas Acesso em: 18 ago. 2021.

_____. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento – Agesic. Disponível em https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/datos-y-estadisticas/estadisticas/estudio-sobre-conocimientos-actitudes-practicas-ciudadania-digital-2020 Acesso em: 18 ago. 2021.

_____. Ley nº 19.948 – Protocolo de Enmienda del Convenio para la Protección de las Personas con Respecto al Tratamiento de Datos Personales. Disponível em https://legislativo.parlamento.gub.uy/temporales/docu2658963172439.htm Acesso em: 22 ago. 2021.

_____. Unidad Reguladora y de Control de Datos Personales – URCDP. Disponível em https://www.gub.uy/unidad-reguladora-control-datos-personales/ Acesso em: 18 ago. 2021.

VASCONCELOS, Beto; DE PAULA, Felipe. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. In: TEPEDINO, Gustavo; FRAZÃO, Ana**; OLIVA, Milena Donato (Coord.).** Lei Geral de Proteção de Dados Pessoais: e suas repercussões no Direito Brasileiro. São Paulo: Revista dos Tribunais, 2019.

WHITMAN, James Q. The Two Western Cultures of Privacy: Dignity versus Liberty. Yale Law Journal. Yale: The Yale Law Journal. v. 113, n. 06, p. 1151-1221, Apr. 2004.

WIMMER, Miriam. Autoridades de Proteção de Dados Pessoais no Mundo: fundamentos e evolução na experiência comparada. In: PALHARES, Felipe (Coord.). Temas Atuais de Proteção de Dados. São Paulo: Revista dos Tribunais, 2020.

II_Outros Estudos

Avaliação de impacto sobre a proteção de dados

Eliseu Filipe Pinto Lopes[212]

INTRODUÇÃO

Facto incontornável da vida nas sociedades modernas é a omnipresença das tecnologias de informação no quotidiano dos cidadãos e a relação de dependência entre estes e aquelas. A velocidade e o impacto das transformações tecnológicas foi avassalador e, em poucas décadas, alterou irreversivelmente o modo de vida e o pensamento dos seres humanos.

Na viragem para o século XXI, a conveniência e as oportunidades proporcionadas pela evolução tecnológica permitiram uma adesão, quase sem reservas, da generalidade dos indivíduos e das organizações a um "*admirável mundo novo*". A massificação da utilização das novas tecnologias como *Apps*, *Smartphone*, *Cloud*, *Internet of Things*, *Inteligência Artificial*, entre outros, veio permitir a recolha de cada vez mais dados pessoais dos cidadãos com o propósito de estabelecer padrões de comportamento e do seu aproveitamento para a exploração comercial. As nossas vidas passaram a depender de tecnologias que nos extraem, mais ou menos secretamente, a nossa experiência privada, traduzida em biliões de dados com que os gigantes tecnológicos alimentam um negócio de milhares de milhões ("*Data is the new oil*"). Esta sistemática expropriação da experiência humana, o imperativo de extração de dados e o processo de transformação do "excedente comportamental" em produtos preditivos suscetíveis de mercantilização e gerador de avultados lucros estão na base daquilo a que Shoshana Zuboff considera a *Era do Capitalismo da Vigilância*[213]. Para a referida investigadora norte-americana o que está em causa é profundamente antidemocrático, considerando que "os capitalistas da vigilância querem manipular o nosso comportamento para que ele se ajuste às suas previsões – uma coerção invisível"[214].

---

[212] Técnico Superior no Alto Comissariado para as Migrações, I.P., pós-graduado em Proteção de Dados Pessoais, Privacidade e Cibersegurança na UE pela Autónoma Academy – Academia de Pós-Graduações da Universidade Autónoma de Lisboa, pós-graduado em Direito do Trabalho e licenciado em Direito pela Universidade Lusíada.

[213] ZUBOFF, Shoshana – A Era do Capitalismo da Vigilância, A disputa por um futuro humano na nova fronteira do poder. Tradução de Luís Filipe Silva e Miguel Serras Pereira. Relógio D'Água Editores, 2020. ISBN 978-989-783-090-7.

[214] ZUBOFF, Shoshana – O Facebook mata. Público. P2. (9 jan. 2022), p. 4-7. Entrevista concedida a Pedro Rios.

Esta preocupação é tanto reforçada quando o que está em causa, não raras vezes, é a utilização de dados de natureza altamente sensível que passam pela dimensão mais íntima ou secreta da pessoa humana (como acontece, entre outros, com os dados de saúde, os registos criminais, a situação financeira, as opiniões políticas ou as convicções religiosas), consubstanciando um forte impacto na vida dos cidadãos.

Uma invasão tão avassaladora da privacidade e uma forte dependência dos serviços e dos produtos tecnológicos por parte dos cidadãos atenta contra as liberdades e ataca a democracia, gerando a perceção de que não há alternativa à morte da privacidade no novo paradigma da "sociedade da vigilância". No sentido de combater tal pensamento insurgem-se vozes como a de Carissa Véliz que, na obra "Privacidade é Poder", preconiza a urgência de, enquanto cidadãos, recuperarmos o controlo dos nossos dados. Defende a autora que chegou o momento de "desligar na tomada" a economia da vigilância e salvar a nossa privacidade. Para alcançar este objetivo coletivo é apontada, entre outras, a exigência de melhor regulamentação junto dos decisores políticos, não só para travar os abusos das grandes corporações na recolha de dados, como também para exigir elevados padrões de cibersegurança na proteção dos dados cujo tratamento esteja legalmente autorizado[215].

A verdade é que, ao longo dos últimos anos, a privacidade e a segurança dos dados pessoais têm assumido um papel de maior relevo no espaço mediático e na opinião pública. Em Portugal, eventos mais recentes, como os ataques informáticos ao grupo Impresa[216], à Vodafone Portugal[217] e aos Laboratórios Germano de Sousa[218], demonstram que mesmo organizações de grande dimensão estão vulneráveis a atividades cibercriminosas que podem envolver a violação de dados pessoais[219] e a respetiva venda na chamada *Dark Web*[220] [221]. Igualmente, o sector público enfrenta desafios relativos à proteção dos dados pessoais dos cidadãos quando se constata que diversos sítios eletrónicos dos serviços públicos de saúde e de justiça disponibilizam indevidamente informação sensível dos utentes para exploração de campanhas publicitárias por parte do Google Analytics[222]. Um outro caso, com bastante

---

[215] VÉLIZ, Carissa – Privacidade é Poder, Por que razão e como devemos recuperar o controlo dos nossos dados. Tradução de Pedro Vidal. Temas e Debates – Círculo de Leitores, 2022. ISBN 978-989-644-688-8, Cap. 5, p. 159-233.

[216] RODRIGUES, José Varela – Impresa avalia "impacto potencial" do ciberataque e toma "medidas necessárias. Dinheiro Vivo. Diário de Notícias. (5 jan. 2022). [Consult. 20 mar. 2022]. Disponível em https://www.dn.pt/media/impresa-avalia-impacto-potencial-do-ciberataque-e-toma-medidas-necessarias-14465275.html.

[217] VELHO, Marta – Vodafone Portugal foi alvo de ataque informático. Jornal de Negócios. (8 fev. 2022). [Consult. 20 mar. 2022]. Disponível em https://www.jornaldenegocios.pt/empresas/detalhe/vodafone-portugal-foi-alvo-de-ataque-informatico.

[218] CORREIA, Gonçalo e CASANOVA, Rui - Laboratórios Germano de Sousa alvo de ataque informático. CUF alerta para "constrangimentos no acesso ao serviço de análises clínicas". Observador. (10 fev. 2022). [Consult. 20 mar. 2022]. Disponível em https://observador.pt/2022/02/10/laboratorios-germano-de-sousa-alvo-de-ataque-informatico/.

[219] NOGUEIRA, Mariana Almeida – Quando o vírus é digital: os maiores ciberataques da História. Visão. Lisboa. (6 jan. 2022), p. 41-45.

[220] RATO, Maria Moreira – Dark Web. E se o seu cartão de crédito estivesse à venda? Jornal i. [sl]. (24 fev. 2022). p. 16-18.

[221] ALVES, Tiago Rodrigues – Pirata vendeu dados de milhões de cartões bancários na Internet. Jornal de Notícias. Porto. (13 abr. 2022), p. 10.

[222] SÉNECA, Hugo – Sites do SNS enviam dados para a Google. Expresso. Lisboa. (25 de jun. 2021), p. 8.

repercussão mediática e social[223], esteve relacionado com a partilha indevida pela Câmara Municipal de Lisboa de dados pessoais de manifestantes e ativistas russos com a Embaixada Russa, o que levou à intervenção da Comissão Nacional de Proteção de Dados (CNPD) que, ao abrigo dos poderes sancionatórios, decidiu aplicar ao Município uma coima única, no valor de um milhão duzentos e cinquenta mil euros[224].

A consciencialização da necessidade de travar ou atenuar as, cada vez maiores e mais sofisticadas, ameaças à privacidade e à segurança dos dados dos cidadãos, evidenciou a importância de uma nova regulamentação que especificasse as medidas adequadas a ter em conta nos tratamentos de dados e as ações e os controlos a levar a cabo pelas organizações para tornar os seus sistemas mais seguros. Por outro lado, procurou-se evitar que os dados pessoais obtidos pelas entidades sejam tratados para finalidade distinta daquela para a qual foram inicialmente recolhidos, garantindo-se o direito de informação dos titulares e de que estes têm conhecimento do que acontece aos seus dados. Daí que, ao nível europeu, foi necessário atualizar o quadro legal da proteção de dados, o que veio a materializar-se com a aprovação do Regulamento Geral da Proteção de Dados (RGPD)[225] que entrou em vigor em 25 de maio de 2016 e se tornou obrigatório em 25 de Maio de 2018, com objetivo de colmatar insuficiências da Diretiva 95/46/CE (D 95/46).

O RGPD, ao contrário da referida Diretiva, deve ser implementado de forma harmonizada em todos os países e assume dois grandes propósitos: defender os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção de dados e promover a livre circulação dos dados pessoais, nos termos do previsto nos n.ºs 2 e 3 do art. 1.º.

Numa verdadeira mudança de paradigma regulatório, o RGPD veio alterar significativamente o quadro das obrigações atribuídas ao responsável pelo tratamento, desde logo, a supressão da necessidade de notificação do tratamento de dados pessoais à autoridade de controlo até então prevista na anterior Diretiva. Em contrapartida, veio estabelecer "um verdadeiro princípio de autorresponsabilização" do responsável pelo tratamento (e subcontratante), atribuindo-lhe outros deveres que o coloca "no papel de vigilante de si mesmo", aqui se incluindo, entre outras, as obrigações de, em determinadas circunstâncias, realizar avaliações de impacto sobre a proteção de dados, manter um registo atualizado dos tratamentos que efetue e ainda, quando aplicável, nomear um Encarregado de Proteção de Dados (EPD)[226].

---

[223] LANÇA, Filomena - Russiagate: Lisboa cometeu 225 infrações com coimas máximas até 20 milhões. Jornal de Negócios. (01 jul. 2021). [Consult. 22 mar. 2022]. Disponível em https://www.jornaldenegocios.pt/economia/detalhe/russiagate-lisboa-cometeu-225-infracoes-com-coimas-maximas-ate-20-milhoes.

[224] Comissão Nacional de Proteção de Dados – Deliberação/2021/1569 aprovada na reunião de 21 de dezembro de 2021. [Em linha]. Lisboa. [Consult. 22 mar. 2022]. Disponível em https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-aplica-sancao-ao-municipio-de-lisboa/.

[225] REGULAMENTO (UE) 2016/679. Jornal Oficial da União Europeia. [Em linha]. (04-05-2016), p. L119/1-119/88. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT.

[226] ANDRADE, Rodrigo Rocha – Da Responsabilidade do Encarregado da Proteção de Dados. Fórum da Proteção de Dados. [Em linha]. N.º 7 (2020), p. 25. [Consult. 28 mar. 2022]. Disponível em https://www.cnpd.pt/media/5kajlbve/forum7_web.pdf.

Importa ainda ter em conta que o RGPD aborda a questão da proteção dos dados de uma forma orientada à gestão do risco. Preconiza-se, com base nas categorias de dados pessoais e nos processos que tratam esses dados, analisar o risco associado aos mesmos e às suas atividades de modo a avaliar efetivamente o risco a que estão sujeitos, permitindo aplicar as medidas técnicas de segurança adequadas para mitigar esses riscos e garantir a proteção dos dados pessoais e os respetivos titulares contra possíveis abusos de informação e ameaças. Pese embora a chamada "abordagem baseada no risco" não seja um conceito novo, pois já decorria da aplicação de alguns preceitos normativos da D 95/46, a verdade é que ganhou relevância nas discussões no Parlamento Europeu e no Conselho sobre a proposta de Regulamento Geral de Proteção de Dados, tendo-se assumido como um elemento central do próprio princípio de responsabilidade e, em especial, na obrigação de realizar uma avaliação de impacto. No debate público sobre a regulamentação da proteção de dados saiu reforçada a ideia de que, em contexto de tratamento de grandes volumes de dados ("big data"), o foco da conformidade legal não se devia restringir à mera recolha dos dados, mas passar a incidir igualmente na utilização que é dada aos dados pessoais, promovendo-se o uso responsável dos dados com base na gestão do risco[227].

Na emergência deste novo paradigma autorregulatório e da inerente reconfiguração do princípio da responsabilidade no RGPD, o objetivo principal deste trabalho centra-se na análise da Avaliação de Impacto sobre a Proteção de Dados (AIPD), enquanto instrumento de *accountability*, na concretização do respetivo regime jurídico e ainda na apresentação de algumas orientações que, esperamos, possam contribuir para a melhor compreensão e aplicação prática deste processo por parte dos sujeitos obrigados à sua realização.

1. OS PRINCÍPIOS APLICÁVEIS AO TRATAMENTO DE DADOS PESSOAIS

O RGPD, no seu Capítulo II, vem estabelecer um conjunto de princípios de respeito obrigatório no tratamento de dados, princípios esses que se constituem como verdadeiros pilares do quadro normativo relativo à proteção de dados pessoais.

Verificou-se um reforço dos princípios já plasmados na D 95/46, assim como a consagração de novos princípios orientadores da conduta dos sujeitos obrigados ao tratamento de dados (responsáveis pelo tratamento, subcontratantes e terceiros), fazendo-se a sua enunciação no artigo 5.º[228] e a concretização do princípio da licitude nos artigos seguintes.

A importância deste acervo normativo reflete-se, desde logo, no teor da redação do direito à proteção dos dados pessoais que se encontra plasmado na Carta dos Direitos Fundamentais da UE, que no n.º 2 do art. 8.º especifica que "os dados devem

[227] Cfr. Article 29 Data Protection Working Party - Statement on the role of a risk-based approach in data protection legal frameworks (14/EN WP218), adotada em 30 de maio 2014. [Em linha]. [Consult. 28 mar. 2022]. Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

[228] Doravante, todas as menções de artigos sem indicação da fonte normativa reportam-se ao Regulamento Geral Sobre a Proteção de Dados (RGPD) – 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.

ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei."

Do mesmo modo, a relevância dos princípios relativos ao tratamento de dados instituídos no RGPD decorre da opção pela sanção mais elevada em caso de violação dos mesmos, a saber, coima até € 20.000.000 ou, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado[229].

1.1 Princípios da "licitude, lealdade e transparência"

Estes três princípios aparecem elencados na al. a) do n.º 1 do artigo 5.º do RGPD. O princípio da licitude, em sentido amplo, exige que o tratamento de dados pessoais ocorra com base no consentimento do titular dos dados ou em outro fundamento previsto na Lei, quer no RGPD quer em outro ato de direito da União ou de um Estado-Membro[230].

No entanto, para A. Barreto Menezes Cordeiro, o RGPD utiliza os termos licitude e ilicitude em sentido mais estrito, ou seja, qualquer tratamento de dados pessoais só será lícito se fundado numa das alíneas do n.º 1 do artigo 6.º (com as densificações previstas nos artigos 7.º e 8.º, relativas ao consentimento) ou numa das alíneas do artigo 9.º ou no artigo 10.º (sempre que o tratamento respeite, respetivamente, a dados pessoais sensíveis ou a dados pessoais relacionados com condenações penais e infrações)[231].

O referido n.º 1 do art. 6.º elenca, de forma taxativa, os fundamentos de licitude do tratamento, estabelecendo que este só é lícito quando o titular dos dados tiver dado o seu consentimento para uma ou mais finalidades específicas, quando for necessário para a execução de um contrato do qual a pessoa singular seja ou venha a ser em breve parte, para o cumprimento de uma obrigação jurídica[232], para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular, para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento, para efeito dos interesses legítimos[233] prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto quando

---

[229] Cfr. al. a) do n.º 5 do artigo 83.º do RGPD.

[230] Considerando 40 do RGPD.

[231] CORDEIRO, A. Barreto Menezes – Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019. Coimbra: Edições Almedina, 2021. ISBN 978-972-40-9261-4. P. 102-103.

[232] O fundamento jurídico do tratamento realizado ao abrigo de uma obrigação jurídica ou quando o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento é definido pelo direito da União ou do Estado-Membro ao qual o responsável pelo tratamento está sujeito (cfr. n.º 3 do art. 6.º do RGPD).

[233] Considerando 47 do RGPD "(...) a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta."

prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção de dados pessoais.

Deste modo, o alcance do texto da lei é claro e indiscutível: "o tratamento só é válido se e na medida em que se verifique pelo menos uma das seguintes situações". O teor dos n.ºs 2 e 3 do referido artigo 6.º não contém qualquer cláusula de abertura que permita aos Estados-Membros ou à União Europeia positivar outros fundamentos de licitude de tratamento de dados. As competências aí consagradas apenas possibilitam concretizações do regime europeu e já não soluções contrárias ou não harmoniosas.

Já no que respeita à escolha do fundamento legal adequado para o tratamento de dados importa referir que a mesma deve ser feita antes do início do tratamento e em relação a uma finalidade específica. Igualmente, o responsável pelo tratamento deve ser coerente na escolha do fundamento legal e tem a obrigação de ser transparente quanto à sua utilização, de modo que se escolheu utilizar o consentimento como fundamento adequado para um determinado tratamento de dados pessoais e o indicou ao titular dos dados[234], não pode *a posteriori* alterar a base legal desse tratamento, se, por exemplo, o titular dos dados retirar o consentimento ou se estiver em causa a validade deste, para continuar a realizar o tratamento em questão. Não pode, portanto, recorrer retroativamente a outro fundamento legal, como o do interesse legítimo, para justificar o tratamento, o que seria fundamentalmente desleal para com o titular dos dados[235].

Acresce que, todos os fundamentos de licitude que legitimam um tratamento, à exceção do relacionado com o consentimento, são expressos como uma necessidade para a realização de uma finalidade específica (seja a execução de um contrato, o cumprimento de uma obrigação jurídica, a defesa de interesses vitais do titular dos dados, o exercício de funções de interesse público ou da autoridade pública ou a prossecução de interesses legítimos do responsável pelo tratamento ou de terceiros). Consequentemente, o GT29 veio notar que esses fundamentos legais estão sempre sujeitos ao chamado "teste de necessidade" que limitará de forma estrita o seu âmbito de aplicação[236].

Naturalmente que, em determinadas situações, o responsável pelo tratamento poderá encontrar diversos fundamentos legais adequados ao tratamento se, por exemplo, uma parte desse tratamento de dados puder ser abrangido pela celebração de contrato com o titular dos dados, mas a outra parte do tratamento exigir o consentimento desse mesmo titular. Significa isto que não está excluída, à partida, a aplicação simultânea de vários fundamentos, desde que sejam aplicados no contexto correto.

O responsável do tratamento que escolha o consentimento como fundamento de licitude do tratamento deve sempre ter em consideração a possibilidade, mais ou menos evidente, do titular dos dados não consentir no respetivo tratamento. Pelo que, não deve ver no consentimento do titular dos dados uma via aberta para legitimar todo

---

[234] Nos termos da al. c) do n.º 1 do artigo 13.º e/ou al. c) do n.º 1 do art. 14.º, o responsável pelo tratamento deve informar o titular dos dados acerca da finalidade e do fundamento jurídico para o tratamento.

[235] GT29 – Orientações relativas ao consentimento na aceção do Regulamento (EU) 2016/679 (WP 259rev.01), 28 nov. 2017, revistas, por último, a 10 abr. 2018, p. 26. No mesmo sentido, nas Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 (versão 1.1) adotadas em 4 de maio de 2020, p. 29.

[236] GT29 – Parecer 15/2011 sobre a definição de consentimento (WP 187), 13 jul. 2011, p. 8.

e qualquer tratamento de dados de um modo expedito e despreocupado. Nesta perspetiva, o responsável pelo tratamento que escolhe um fundamento legal inadequado encontra-se numa posição de falsa sensação de segurança em relação à licitude do tratamento que se pode desfazer a qualquer momento. O consentimento deve ser, por isso, o fundamento legal a que se pode recorrer quando nenhum dos outros legalmente previstos se revele adequado ao tratamento de dados que se pretende realizar.

O GT29 avança ainda com um critério adicional no que respeita à possibilidade de escolher ou não o consentimento para legitimar o tratamento de dados pessoais e que se prende com a natureza do responsável pelo tratamento. Este é o caso dos responsáveis pelo tratamento inseridos no setor público em que, normalmente, o tratamento de dados radica no cumprimento de obrigação legal ou na execução de uma missão de interesse público. Pelo que, nestes casos, o consentimento do titular dos dados não é o fundamento legal adequado para legitimar o tratamento de dados em causa[237].

No mesmo sentido, D. Francisco e S. Francisco esclarecem que "na existência de uma missão de interesse público ou levada a cabo no interesse de uma autoridade pública, as Entidades Públicas, desde que devidamente legitimadas por lei (da U.E. ou de Portugal), possuem licitude para efetuar tratamento de dados pessoais sem necessidade de consentimento do titular dos dados (a pessoa singular)" (p.34)[238].

O princípio da lealdade encontra-se, intrínseca e diretamente, ligado com a transparência do tratamento, devendo a conduta do responsável pelo tratamento ser orientada pelo escrupuloso cumprimento do RGPD. A concretização deste princípio impõe que os tratamentos realizados pelos responsáveis pelo tratamento se guiem por critérios equitativos[239] e ainda que, na relação individual estabelecida com os titulares dos dados, aqueles responsáveis tenham o dever de atenderem, a todo o tempo, aos interesses e expectativas legítimas dos referidos titulares[240].

Por sua vez, o princípio da transparência apresenta-se como novidade do RGPD[241] e "atravessa, horizontalmente, todo o processo de tratamento de dados, desde os primeiros contatos que o responsável pelo tratamento estabelece com potenciais titulares de dados (formação), passando pela sua recolha e demais tratamentos (execução), conservando-se mesmo após o termo da relação"[242].

Neste sentido, o Considerando 39[243] estabelece que o tratamento deverá ser realizado de forma transparente de modo a que os titulares dos dados tenham pleno

---

[237] GT29 – Parecer 15/2011, Op. Cit. p. 17.

[238] FRANCISCO, Daniel e FRANCISCO, Sandra – Regulamento Geral de Proteção de Dados: 7 passos para uma metodologia de implementação do RGPD na Administração Pública. Lisboa. Edições Sílabo, 2019. 1ª Edição. ISBN 978-989-561-014-3. P. 34.

[239] A expressão "tratamento equitativo" é utilizada no n.º 2, do art. 13.º e al. a) do n.º 2 do art. 40.º do RGPD e nos seus Considerandos 39, 60 e 71 para densificar o conceito de lealdade.

[240] CORDEIRO, A. Barreto Menezes – Op. Cit. p. 103.

[241] Considerando 39 do RGPD; GT29 – Orientações relativas à transparência na aceção do Regulamento 2016/679 (WP 260rev.1), 29 nov. 2017, revistas, por último, a 11 abr. 2018.

[242] CORDEIRO, A. Barreto Menezes – Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2019. Coimbra: Edições Almedina, março de 2020. Reimpressão. ISBN 978-972-40-8304-9. P. 154-155.

[243] Doravante, todas as menções a Considerandos sem indicação da fonte normativa reportam-se ao Regulamento Geral Sobre a Proteção de Dados (RGPD) – Regulamento (UE) 2016/679 do Parlamento

conhecimento dos dados pessoais que são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento, assim como a medida em que os dados são ou virão a ser tratados, implicando que as informações e as comunicações transmitidas ao titular dos dados seja feita numa linguagem clara e simples, permitindo o seu fácil acesso e compreensão.

Por sua vez, o Considerando 58 vem prever que o princípio da transparência exige que qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado.

O GT29 esclarece que "a transparência é uma obrigação abrangente nos termos do RGPD aplicável a três domínios centrais: 1) o fornecimento de informações aos titulares dos dados relacionado com o tratamento leal; 2) de que forma os responsáveis pelo tratamento comunicam com os titulares dos dados em relação aos direitos destes ao abrigo do RGPD; e 3) de que forma os responsáveis pelo tratamento facilitam o exercício dos direitos dos titulares dos dados"[244].

Como bem se evidencia, o princípio da transparência, ainda que com particular incidência na matéria, não se esgota no estrito exercício do direito à informação dos titulares dos dados pessoais, tendo, aliás, concretização em inúmeros artigos do RGPD, com destaque para os artigos 12.º, 13.º e 14.º, mas também nos artigos 34.º ou 37.º.

1.2 Princípio da "limitação das finalidades"

Este princípio pressupõe uma limitação do tratamento à finalidade inicialmente determinada pelo responsável pelo tratamento. O disposto na al. b) do n.º 1 do artigo 5.º limita a recolha de dados pessoais a finalidades (i) determinadas, (ii) explícitas e (iii) legítimas. O fundamento constitucional deste princípio encontra-se no já citado n.º 2 do artigo 8.º da Carta dos Direitos Fundamentais da EU na referência aos "fins específicos".

Significa isto que ao responsável pelo tratamento está vedada a prossecução de tratamentos de dados pessoais incompatíveis com as finalidades originalmente indicadas. Tais finalidades devem ser definidas antes do processo de tratamento se iniciar (determinadas), informadas aos titulares dos dados e conhecidas dos interessados (explícitas) e cumpridoras de todas as disposições legais em concreto aplicáveis (legítimas)[245].

A este propósito, o GT29 esclarece que, para estarmos perante finalidades devidamente determinadas, não basta a utilização de expressões vagas ou genéricas como: "melhorar a experiência dos utilizadores", "fins publicitários" ou "segurança cibernética"[246].

O princípio da limitação das finalidades assume especial relevância na medida em que permite que o titular dos dados, ao disponibilizar os seus dados, tenha pleno conhecimento das finalidades para as quais os seus dados serão tratados, limitando tratamentos para finalidades diversas das quais os dados pessoais tenham sido

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.

244 GT29 – Orientações relativas à transparência na aceção do Regulamento 2016/679 (WP 260rev.1), 29 nov. 2017, revistas, por último, a 11 abr. 2018, p. 4.

245 CORDEIRO, A. Barreto Menezes – Comentário, Op. Cit. p. 104.

246 GT29 – Opinion 03/2013 on purpose limitations (WP 203), 2 abr. 2013, p. 16.

inicialmente recolhidos, dispondo a al. b) do n.º 1 do artigo 5.º que os dados pessoais devem ser recolhidos para "finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de modo incompatível com essas finalidades"[247].

Para aferir a compatibilidade de uma nova finalidade com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, o teor do Considerando 50 faculta algumas pistas ao esclarecer que o responsável pelo tratamento deverá atentar à existência de uma ligação entre a finalidade primordial e a nova finalidade a que se destina a operação de tratamento que pretende levar a cabo, o contexto em que os dados pessoais foram recolhidos, "em especial as expetativas razoáveis do titular dos dados quanto à sua posterior utilização, baseadas na sua relação com o responsável pelo tratamento, a natureza dos dados pessoais, as consequências que o posterior tratamento dos dados pode ter para o seu titular e a existência de garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas"[248].

Segundo A. Barreto Menezes Cordeiro o conteúdo do Considerando 50 é, aparentemente, contraditório: "O tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais". Contudo, uma leitura mais atenta mostra que não se aplica aos casos em análise: é empregue a expressão "se for compatível" e não "se não for incompatível". *A contrario sensu* podemos concluir que todas as finalidades e tratamentos compatíveis com as indicadas pelo responsável pelo tratamento não necessitam de qualquer controlo extraordinário[249].

Alguma doutrina considera que o princípio da limitação das finalidades terá um grande impacto nos modelos de "*big data*". A este propósito afirmam Noronha Rodrigues e Medeiro Teves: «Ghani, Hamid & Udzir (2016) consideram que o "*big data* desafia o princípio da limitação das finalidades, e o princípio é uma barreira ao desenvolvimento da análise de *big data* (…) tendo um impacto negativo na eficiência do modelo "aviso e consentimento", uma vez que "as análises de *big data* permitem uma análise de dados usando algoritmos diferentes, o que revela correlações inesperadas que podem ser usadas para novos propósitos. O princípio da limitação das finalidades restringe a liberdade de uma organização fazer essas descobertas e inovações"(p. 116-121)»[250].

---

[247] Nos termos do n.º 1 do artigo 89.º do RGPD os tratamentos posteriores para finalidades de arquivo de interesse público, investigação científica ou histórica ou para efeitos estatísticos deverão ser considerados tratamentos compatíveis com as finalidades que legitimaram a recolha de dados e lícitos.

[248] Artigo 6.º número 4 do RGPD.

[249] CORDEIRO, A. Barreto Menezes – Comentário, Op. Cit. p. 105.

[250] RODRIGUES, José Noronha e TEVES, Daniela Medeiros, apud, GANI, N. A., HAMID, S. e UDZIR, N. I. PEREIRA – Big Data and Data Protection: Issues with Purpose Limitation Principle. International Journal of Advances in Soft Computing na Its Appication, 8(3), p. 116-121.

1.3 Princípio da "minimização de dados"

O princípio da "minimização de dados" encontra-se previsto na al. c) do n.º 1 do artigo 5.º e surge intrinsecamente associado ao princípio da limitação das finalidades: os dados pessoais devem ser "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados".

A adequação impõe a circunscrição dos tratamentos aos dados pessoais que se enquadrem nas finalidades prosseguidas. Ficam, por isso, excluídos *ab initio* os dados não relacionados ou excluídos. A pertinência delimita as atividades dos responsáveis a tratamentos que possam contribuir para a prossecução dessas finalidades. Por último, importa ter em conta que o tratamento apenas será juridicamente admissível se não existir um método alternativo menos intrusivo dos direitos dos titulares, como por exemplo a anonimização (al. a) do n.º 1 do artigo 32.º) ou a pseudonimização (n.º 1 do artigo 25.º)[251].

Pela aplicação deste princípio proíbe-se a recolha junto dos titulares de mais dados pessoais do que aqueles que são necessários e suficientes para a finalidade de tratamento, remetendo-se o responsável pelo tratamento para uma atuação na base do conceito "*need to know*". Nesta perspetiva, e à semelhança do princípio da limitação das finalidades, o princípio em análise é apontado como um desafio aos modelos de "*big data*", na medida em que as organizações, enquanto responsáveis pelo tratamento, são obrigadas a limitar a recolha de dados pessoais ao necessário para atingir os seus objetivos legítimos e a eliminar os que não estão de acordo com esses propósitos[252].

1.4 Princípio da "exatidão"

Plasmado na al. d) do n.º 1 do art. 5.º, o princípio da "exatidão" impõe que os dados pessoais objeto de tratamento devem ser exatos e atualizados, devendo os dados inexatos, considerando as finalidades para as quais são tratados, ser apagados ou retificados.

Subdivide-se, por isso, em três dimensões: (i) a proibição de recolher ou armazenar dados incorretos; (ii) o dever de atualização dos dados detidos, sempre que se mostre necessário; e (iii) o dever de apagar ou retificar os dados incorretos, à luz das finalidades prosseguidas[253].

De salientar que a obrigação de apagar ou de retificar dados incorretos não se confunde com os direitos do titular dos dados a exigir o apagamento dos dados (independentemente de serem incorretos ou não) – art. 17.º, ou da sua retificação – art. 16.º.

---

[251] CORDEIRO, A. Barreto Menezes – Comentário, Op. Cit. p. 105.

[252] RODRIGUES, José Noronha e TEVES, Daniela Medeiros, Op. Cit. p. 53.

[253] CORDEIRO, A. Barreto Menezes – Direito, Op. Cit. p. 159.

1.5 Princípio da "limitação da conservação"

Este princípio delimita a conservação dos dados pessoais, vedando a possibilidade de conservações por tempo indeterminado. Quer isto significar que os dados pessoais dos titulares só podem ser conservados durante o tempo necessário para a prossecução da finalidade para a qual foram recolhidos e são tratados. Findo esse período de tempo os dados devem ser, o quanto antes, apagados.

A al. e) do n.º 1 do artigo 5.º estipula as regras relativas à conservação, determinando que os dados pessoais devem ser conservados de forma que "permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos (…), sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados".

Compete ao responsável pelo tratamento fixar os prazos para o apagamento dos dados ou para a revisão periódica da sua conservação, de forma a assegurar que os dados pessoais sejam mantidos apenas durante o período de tempo indispensável[254]. Caso não seja possível fixar um prazo determinado, deverá o responsável pelo tratamento, pelo menos, enunciar os critérios para a sua fixação (prazo indeterminado mas determinável), conforme previsto no direito à informação (al. a) do n.º 2 do artigo 13.º e al. a) do n.º 2 do artigo 14.º), no direito de acesso (al. d) do n.º 1 do artigo 15.º), no direito ao apagamento (al. a) do n.º 1 do artigo 17.º), no direito à limitação (n.º 1 do artigo 18.º) e no dever de registo dos prazos de conservação (al. f) do n.º 1 do artigo 30.º) ou mesmo em matéria de *privacy by default* (n.º 2 do artigo 25.º)[255]. A densificação desta obrigação encontra-se no artigo 21.º da Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do RGPD, doravante designada de Lei de Execução (LE).

1.6 Princípios da "integridade e da confidencialidade"

Elencados na al. f) do n.º 1 do artigo 5.º, estes dois princípios impõem que os dados pessoais devem ser "tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas".

Aparecem com o RGPD na medida em que não têm paralelo na anterior D 95/46. O preceito em causa vem estabelecer obrigações acrescidas aos responsáveis pelo tratamento, concretamente as de garantirem a segurança e a confidencialidade dos dados. A segurança abrange a perda, a destruição ou a danificação acidental, independentemente do impacto total ou parcial. A confidencialidade abarca tratamentos não autorizados.

---

[254] Considerando 40 do RGPD.

[255] CORDEIRO, A. Barreto Menezes – Comentário, Op. Cit. p. 603.

Pelo que, constitui obrigação dos responsáveis pelo tratamento adotar as medidas técnicas e organizativas adequadas a garantir o cumprimento de ambos os princípios que têm ampla densificação no artigo 32.º do RGPD. Portanto, deve-se entender que, pese embora apenas as dimensões de segurança relativas à integridade e à confidencialidade sejam mencionadas, também há que que ter em linha de conta a garantia de disponibilidade dos dados, especificada neste preceito.

1.7 Princípio da "responsabilidade"

O princípio da "responsabilidade" vem enunciado no n.º 2 do artigo 5.º e estabelece que "o responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo".

Desde logo, verifica-se, pela localização sistemática, que se trata de um princípio que difere dos restantes princípios, pois aparece autonomizado num número à parte e reporta-se justamente aos demais. Este aspeto poderia suscitar dúvidas quanto à sua consideração como princípio, não fosse o facto de estar integrado no artigo 5.º sob a epígrafe "Princípios relativos ao tratamento de dados pessoais" que, por sua vez, abre o Capítulo II do RGPD sob a designação "Princípios".

Da forma como se encontra positivado, o princípio da responsabilidade consubstancia uma novidade do RGPD. Este princípio opera a dois níveis: (i) o responsável pelo tratamento deve atuar sempre no estrito cumprimento dos princípios elencados no n.º 1 do artigo 5.º; e (ii) o responsável pelo tratamento deve conseguir demonstrar, *maxime* às autoridades de controlo e aos tribunais, o cumprimento desses princípios[256]. É precisamente este segundo nível que reveste maior novidade no RGPD que, no n.º 1 do seu artigo 24.º, vem estabelecer que "tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis", cabe ao responsável pelo tratamento aplicar "as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o regulamento".

Foi pela primeira vez introduzido no contexto da proteção de dados, a nível internacional, nas *Guidelines* da OCDE, adotadas em 23 de setembro de 1980[257]. A partir dessa data, a importância deste princípio tem vindo a ser discutida em inúmeros fóruns internacionais dedicados à matéria de proteção de dados. Em especial, destaca-se o Parecer 3/2010 sobre o princípio da responsabilidade[258], emitido pelo GT29, no qual foi defendida a introdução deste princípio na revisão do regime geral de proteção de dados, com o objetivo de reafirmar e reforçar a responsabilidade do responsável pelo tratamento.

Ainda que positivada no RGPD a obrigação de demonstração de cumprimento, o legislador europeu não esclarece de que forma o cumprimento dos princípios do n.º

---

256 CORDEIRO, A. Barreto Menezes – Comentário, Op. Cit. p. 106.

257 OCDE - Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. [Em linha]. Disponível https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1648644605&id=id&accname=guest&checksum=DC0AE8ED7821150A25BCD3DF6A4EF883

258 GT29 – Parecer 3/2010 sobre o princípio da responsabilidade (WP 173), 13 de Jul. de 2010. [Em Linha]. Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_pt.pdf.

1 do artigo 5.º pode ser comprovado. Na esteira do citado Parecer 3/2010 do GT29, vingou a necessidade de prever uma certa flexibilidade e adaptabilidade de regime, deixando em aberto a possibilidade de cada responsável pelo tratamento poder adaptar as medidas às características concretas dos dados pessoais e das operações de tratamento em questão.

Com efeito, de acordo com o princípio da responsabilidade, as medidas técnicas e organizativas a adotar pelos responsáveis pelo tratamento deverão ser determinadas em função dos factos e circunstâncias de cada caso em particular, incluindo o tipo de operações de tratamento de dados e os riscos para os direitos e liberdades das pessoas singulares. Mais concretamente, deverão ser tidos em conta aspetos como a dimensão da operação de tratamento de dados, a sua finalidade, a necessidade de transferência de dados, o tipo de dados que vão ser tratados, incluindo o tratamento de dados pessoais sensíveis[259].

A este propósito o GT29 avança mesmo com situações concretas quando indica que, "em casos mais complexos, como por exemplo a utilização de dispositivos biométricos inovadores, o cumprimento da «obrigação de demonstração» pode exigir ainda mais requisitos. O responsável pelo tratamento dos dados pode ter de demonstrar por exemplo que realizou uma avaliação de impacto sobre a privacidade, que os colaboradores envolvidos no tratamento recebem formação e são informados regularmente, etc"[260].

No entanto, ao longo do RGPD, não faltam pistas acerca de medidas possíveis, nomeadamente, quando se incentiva a adoção, por parte do responsável pelo tratamento, de políticas internas adequadas em matéria de proteção de dados, assim como o cumprimento de códigos de conduta e procedimentos de certificação, que poderão ser utilizados "como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento" (art. 24.º, n.º 2 e 3).

Podemos, de facto, encontrar no RGPD um conjunto, não exaustivo, de medidas técnicas e organizativas destinadas a assegurar e demonstrar, por parte do responsável pelo tratamento, o cumprimento das regras de proteção de dados. Algumas destas medidas consistem na avaliação de impacto sobre a proteção de dados e consulta prévia, registo das atividades de tratamento (RAT), notificação de violação de dados pessoais, nomeação de um encarregado da proteção de dados, cuja implementação poderá variar, tal como anteriormente referido, consoante o tipo de tratamento de dados e os respetivos riscos para os titulares dos dados. O não cumprimento de qualquer uma destas obrigações, poderá implicar, para cada um dos atos, a aplicação de uma coima até € 10.000.000 ou, no caso de uma empresa, até 2% do seu volume de negócios anual (art. 83.º, n.º 4 do RGPD).

Assim, a avaliação de impacto sobre a proteção de dados aparece como um instrumento que o responsável pelo tratamento tem ao seu dispor para a materialização do princípio da responsabilidade, nomeadamente, do segundo nível, isto é, a demonstração de cumprimento ou daquilo que na versão inglesa do RGPD se denomina de *accountability*.

---

[259] GT29 – Parecer 3/2010. Op. Cit. p. 14

[260] Idem – Ibidem, p. 15.

Cumpre, por isso, salientar que estamos perante aquilo a que a doutrina considera ser uma "responsabilidade proactiva", ou seja, que a obrigação de demonstrar o cumprimento das regras de proteção de dados é suscetível de influenciar um comportamento mais pró-ativo por parte dos responsáveis pelo tratamento, não só no que respeita à implementação de medidas eficazes de proteção de dados nos seus processos de negócio, como também no que concerne à adotação de mecanismos que permitem a avaliação das referidas medidas antes da necessidade de ocorrência de incidentes[261]. Trata-se, efetivamente, de uma mudança de perspetiva sobre a proteção de dados, mediante a passagem de um modelo passivo a um ativo, com especial incidência na atuação do responsável pelo tratamento.

Pelo que, a demonstração pró-ativa da capacidade de uma organização de cumprir, em observância do princípio da responsabilidade, confere, por esta via, uma maior confiança aos titulares dos dados pessoais e reguladores de que as garantias adequadas à proteção dos dados são implementadas.

2. AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

2.1 Conceito e base legal

O RGPD não define formalmente o conceito de uma AIPD[262] propriamente dita, apenas especifica as circunstâncias que obrigam à sua realização e o seu conteúdo mínimo. No entanto, nas "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679", o GT29 expressa que "uma AIPD é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos"[263].

A AIPD é, em termos de legislação europeia em matéria de proteção de dados, uma das inovações introduzidas pela entrada em vigor do RGPD e consubstancia, como acima se expôs, uma decorrência do princípio da responsabilidade previsto no n.º 2 do artigo 5.º, na medida em que ajuda os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas adequadas para assegurar a conformidade com o Regulamento. Como bem sintetiza o GT29, uma AIPD é um processo que visa estabelecer e demonstrar conformidade[264].

---

[261] LOPES, Teresa Vale – Responsabilidade e Governação das Empresas no Âmbito do Novo Regulamento de Proteção de Dados. Anuário da Proteção de Dados 2018. Lisboa, 2018. [Em linha]. p. 54. [Consult. 7 mar. 2022]. Disponível em http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf.

[262] A designação AIPD na versão portuguesa tem correspondência na terminologia anglo-saxónica para a Europa de Data Protetion Impact Assessment (DPIA) ou no continente americano a Privacy Impact Assessment (PIA), utilizando neste último caso o termo "Privacy" em vez de "Data Protetion".

[263] GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679. (WP 248rev.01), 4 abr. 2017, revistas, por último, a 11 out. 2017, p. 4.

[264] Idem – Ibidem.

De acordo com o n.º 1 do artigo 35.º, deve sempre ser realizada uma AIPD para todas atividades de tratamento de dados que possivelmente resultem num risco elevado para os direitos e liberdades dos titulares dos dados, tendo em conta a natureza, âmbito, contexto e propósitos do tratamento.

Logo por aqui se constata que não se pretendeu generalizar a obrigatoriedade de realização da AIPD a todos os tratamentos de dados pessoais, mas limitar a sua incidência aos tratamentos cujo nível de risco se estime como elevado. Neste sentido, para determinar o nível de risco, deverá ser realizada uma análise de risco prévia, dando assim cumprimento à exigência prevista no artigo 24.º.

Por forma a assegurar uma interpretação coerente das circunstâncias em que é obrigatório realizar uma AIPD (artigo 35.º, n.º 3), as referidas orientações do GT29 visam clarificar esta noção e fornecer critérios para as listas a adotar pelas autoridades responsáveis pela proteção de dados nos termos do artigo 35.º, n.º 4.

2.2 Sujeitos obrigados

O responsável pelo tratamento é aquele que tem a obrigação de garantir a realização da avaliação de impacto (n.º 2 do artigo 35.º). Ainda que possa confiar esta tarefa a outras pessoas, dentro ou fora da organização, continua a ser o responsável último pela sua realização.

O responsável pelo tratamento deve também solicitar o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado, sendo que o seu parecer e as decisões tomadas pelo responsável pelo tratamento devem ser documentadas na AIPD[265].

No quotidiano das organizações, não raras vezes, o responsável pelo tratamento, na tentativa de superar insuficiências técnicas ou organizativas próprias, procura "delegar" ou transmitir a obrigação de realização da AIPD ao encarregado da proteção de dados, o que viola frontalmente o RGPD onde os papéis destas duas figuras são distintos e encontram-se bem definidos. Ao encarregado da proteção de dados, como veremos mais à frente, incumbe apenas controlar a realização da AIPD (artigo 39.º, n.º 1, alínea c).

Se o tratamento for total ou parcialmente efetuado por um subcontratante, o subcontratante deve auxiliar o responsável pelo tratamento na realização da AIPD e fornecer todas as informações necessárias (em consonância com o artigo 28.º, n.º 3, alínea f).

Se a operação de tratamento envolve responsáveis conjuntos pelo tratamento, estes devem definir pormenorizadamente as respetivas obrigações. A AIPD deve definir qual das partes é responsável pelas várias medidas concebidas para dar resposta aos riscos e proteger os direitos e as liberdades dos titulares dos dados.

2.3 Âmbito temporal

De acordo com o disposto no n.º 1 do art. 35.º a AIPD deve ser efetuada "antes de iniciar o tratamento". De resto, tal menção está em consonância com a utilização da expressão "antes das atividades de tratamento" prevista no n.º 10 do mesmo preceito e é compatível com o arco temporal a que se reporta o n.º 1 do art. 25.º quando refere

[265] GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, Op. Cit. p. 17.

"no momento da definição dos meios de tratamento". No mesmo sentido, o Considerando 90 quando refere "(…) o responsável pelo tratamento deverá proceder, antes do tratamento, a uma avaliação do impacto sobre a proteção de dados (…)."

O GT29 considera, a este respeito, que a AIPD deve ser encarada como um instrumento de apoio à tomada de decisão em relação ao tratamento. Neste sentido, a AIPD deve ser iniciada o mais cedo possível na conceção da operação de tratamento, mesmo que algumas das operações de tratamento ainda sejam desconhecidas[266].

2.4 Objeto

Uma AIPD pode abranger uma única operação de tratamento ou um conjunto de operações de tratamento semelhantes. Esta segunda possibilidade é confirmada pelo teor do n.º 1 do artigo 35.º quando estabelece que "(…) um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação". Nesse mesmo sentido, o Considerando 92 acrescenta que "em certas circunstâncias pode ser razoável e económico alargar a avaliação de impacto sobre a proteção de dados para além de um projeto único, por exemplo se as autoridades ou organismos públicos pretenderem criar uma aplicação ou uma plataforma de tratamento comum, ou se vários responsáveis pelo tratamento planearem criar uma aplicação ou um ambiente de tratamento comum em todo um setor ou segmento profissional, ou uma atividade horizontal amplamente utilizada".

Assim, uma única AIPD pode ser utilizada para avaliar múltiplas operações de tratamento que sejam semelhantes em termos de natureza, âmbito, contexto, finalidade e riscos. Efetivamente, como bem salienta o GT29, as AIPD visam estudar sistematicamente novas situações que possam ser suscetíveis de implicar riscos elevados para os direitos e as liberdades das pessoas singulares, não havendo necessidade de realizar uma AIPD para os casos que já foram estudados (ou seja, operações de tratamento realizadas num contexto específico e com uma finalidade específica). Verifica-se essa situação quando uma tecnologia semelhante seja utilizada para recolher os mesmos tipos de dados para os mesmos fins[267]. Pode também ser aplicável a operações de tratamento semelhantes aplicadas por vários responsáveis pelo tratamento de dados. Nestes casos, deve ser partilhada ou disponibilizada ao público uma AIPD de referência, devem ser adotadas as medidas descritas na AIPD e deve ser fornecida uma justificação para a realização de uma única AIPD.

Nos casos em que uma operação de tratamento envolve responsáveis conjuntos pelo tratamento, estes devem determinar em concreto as respetivas obrigações, podendo recorrer à celebração de acordos de tratamento de dados. Nestes casos, a AIPD relativa ao tratamento de dados deverá refletir qual das partes é responsável pelas várias medidas aplicadas para dar resposta aos riscos e proteger os

---

[266] GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, Op. Cit. p. 17.

[267] GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, Op. Cit. p. 8. A este propósito é dado o exemplo de um grupo de autoridades municipais, em que cada uma dessas autoridades esteja a instalar um sistema de televisão em circuito fechado (CCTV) semelhante, pode realizar uma única AIPD que abranja o tratamento por parte destes responsáveis pelo tratamento independentes, ou então um operador ferroviário (responsável único) pode abranger a vigilância vídeo em todas as suas estações ferroviárias com uma única AIPD.

direitos e as liberdades dos titulares dos dados. Neste domínio, cada responsável deve colaborar com os demais no sentido de dar conta das suas necessidades e partilhar informações úteis sem comprometer segredos (p. ex.: proteção de segredos comerciais, propriedade intelectual, informações empresariais confidenciais) ou revelar vulnerabilidades.

O GT29 clarifica ainda que uma AIPD também pode ser útil para avaliar o impacto na proteção de dados de um produto tecnológico, por exemplo, um equipamento ou um programa informático, sempre que este seja suscetível de ser utilizado por diferentes responsáveis pelo tratamento de dados para realizar diferentes operações de tratamento. Neste caso, o responsável pelo tratamento de dados que lança o produto continua obrigado a realizar a sua própria AIPD em relação à implementação específica, mas esta pode basear-se em informações de uma AIPD preparada pelo fornecedor do produto, se adequado. A este propósito, o GT29 fornece, a título de exemplo, a relação entre os fabricantes de contadores inteligentes e as empresas de serviços públicos. Cada fornecedor ou subcontratante do produto deve partilhar informações úteis sem comprometer segredos e sem criar riscos de segurança divulgando vulnerabilidades[268].

2.5 Casos de realização obrigatória

Como acima se expôs, o RGPD não exige a realização de uma AIPD para todas as operações de tratamento que possam implicar riscos para os direitos e as liberdades das pessoas singulares. A realização de uma AIPD é obrigatória somente quando o tratamento for "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (artigo 35.º, n.º 1, ilustrado pelo artigo 35.º, n.º 3, e complementado pelo artigo 35.º, n.º 4). O legislador da U.E. adianta um exemplo em particular que se prende com o tipo de tratamento "que utilize novas tecnologias". Outros exemplos surgem nos Considerandos 89 e 91. O requisito do elevado risco surge também no n.º 1 do artigo 34.º relativo à comunicação ao titular dos dados.

Ainda que possa ser necessário realizar uma AIPD noutras circunstâncias, o artigo 35.º, n.º 3, prevê alguns exemplos de quando é que uma operação de tratamento é suscetível de implicar elevados riscos (e como tal, de realização obrigatória da AIPD), como sucede nos casos de:

- "a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar[269];

[268] GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, Op. Cit. p. 9.

[269] Cfr. Considerando 71: "em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis".

- b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º[270]; ou

- c) Controlo sistemático de zonas acessíveis ao público em grande escala."

Conforme se depreende da utilização da expressão "nomeadamente em caso de" na parte introdutória do n.º 3 do artigo 35.º, o elenco apresentado é meramente exemplificativo de três situações em que se presume de forma inilidível existir "elevado risco"[271]. Pelo que podem existir operações de tratamento de "elevado risco" que não estejam incluídas neste elenco, mas que, ainda assim, impliquem riscos elevados. Estas operações de tratamento também devem estar sujeitas a AIPD[272].

No sentido de fornecer um conjunto mais concreto de operações de tratamento que exigem uma AIPD devido ao elevado risco inerente, tendo em conta os elementos específicos dos artigos 35.º, n.º 1, e 35.º, n.º 3, alíneas a) a c), a lista a adotar a nível nacional nos termos do artigo 35.º, n.º 4, e dos considerandos 71, 75 e 91, e outras referências no RGPD a operações de tratamento "suscetível de implicar um elevado risco", o GT29[273] sistematizou nove critérios a ter em conta e que aqui se transcrevem:

1. Avaliação ou classificação, incluindo definição de perfis e previsão, em especial de "aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados" (considerandos 71 e 91)[274];
2. Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar: tratamento destinado à tomada de decisões sobre os titulares dos dados e que produza "efeitos jurídicos relativamente à pessoa singular" ou que "a afetem significativamente de forma similar" (artigo 35.º, n.º 3, alínea a));
3. Controlo sistemático: tratamento utilizado para observar, monitorizar ou controlar os titulares dos dados, incluindo dados recolhidos através de redes, ou um «controlo sistemático de zonas acessíveis ao público» (artigo 35.º, n.º 3, alínea c))[275]. Este tipo de controlo é um critério porque os dados pessoais podem ser

---

[270] Cfr. Considerando 75: "quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas".

[271] CORDEIRO, A. Barreto Menezes – Comentário, Op. Cit. p. 282.

[272] GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, Op. Cit. p. 10.

[273] Idem – Op. Cit. p. 10-12.

[274] O GT29 adianta como exemplos deste critério: uma instituição financeira que faça um controlo seletivo dos seus clientes a partir de uma base de dados de referências de crédito bancário ou a partir de uma base de dados de combate ao branqueamento de capitais e ao financiamento do terrorismo ou de combate à fraude; uma empresa de biotecnologia que ofereça testes genéticos diretamente aos seus clientes por forma a avaliar e prever riscos de doença ou para a saúde; ou uma empresa de desenvolva perfis comportamentais ou publicitários baseados na utilização ou navegação no seu sítio web.

[275] O GT29 interpreta "sistemático" como significando um ou mais dos seguintes pontos (ver as orientações do Grupo de Trabalho do Artigo 29.º sobre o encarregado da proteção de dados 16/EN WP 243): (i) que ocorre de acordo com um sistema; (ii) pré-determinado, organizado ou metódico; (iii) que acontece como parte de um plano geral de recolha de dados; iv) realizado como parte de uma estratégia. O GT29

recolhidos em circunstâncias em que os titulares dos dados podem não estar cientes de quem está a recolher os seus dados e da forma como esses dados serão utilizados. Adicionalmente, pode ser impossível para os indivíduos evitarem estar sujeitos a este tipo de tratamento em espaço(s) público(s) (ou zonas acessíveis ao público);

4. Dados sensíveis ou dados de natureza altamente pessoal: inclui categorias especiais de dados pessoais, tal como definido no artigo 9.º (por exemplo, informações acerca das opiniões políticas dos indivíduos), bem como dados pessoais relacionados com condenações penais e infrações, tal como definido no artigo 10.º[276]. Para além destas disposições do RGPD, algumas categorias de dados podem ser consideradas como categorias que aumentam os possíveis riscos para os direitos e as liberdades dos indivíduos. Estes dados pessoais são considerados sensíveis (na aceção comum deste termo) porque estão associados a atividades privadas e familiares (tais como comunicações eletrónicas cuja confidencialidade deve ser protegida) ou porque afetam o exercício de um direito fundamental (tais como dados de localização cuja recolha põe em causa a liberdade de circulação) ou porque a sua violação implica claramente que a vida quotidiana do titular dos dados será gravemente afetada (tais como dados financeiros que possam ser utilizados numa fraude de pagamentos);
5. Dados tratados em grande escala: o RGPD não define o que constitui grande escala, contudo o Considerando 91 fornece alguma orientação. Em qualquer caso, o GT29 recomenda que os seguintes fatores, em especial, sejam considerados quando se determina se o tratamento é ou não efetuado em grande escala: (i) o número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente; (ii) o volume de dados e/ou a diversidade de dados diferentes a tratar; (iii) a duração da atividade de tratamento de dados ou a sua pertinência; (iii) a dimensão geográfica da atividade de tratamento.
6. Estabelecer correspondências ou combinar conjuntos de dados: por exemplo, com origem em duas ou mais operações de tratamento de dados realizadas com diferentes finalidades e/ou por diferentes responsáveis pelo tratamento de dados de tal forma que excedam as expectativas razoáveis do titular dos dados;
7. Dados relativos a titulares de dados vulneráveis (Considerando 75): o tratamento deste tipo de dados constitui um critério devido ao acentuado desequilíbrio de poder entre os titulares dos dados e o responsável pelo tratamento dos dados, significando isto que os indivíduos podem não ser capazes de consentir, ou opor-se, facilmente ao tratamento dos seus dados ou de exercer os seus direitos. Os titulares de dados vulneráveis podem incluir crianças (estas podem ser consideradas incapazes de consentir ou opor-se consciente e criteriosamente ao tratamento dos seus dados), empregados, segmentos mais vulneráveis da

interpreta "zona acessível ao público" como sendo qualquer local aberto a qualquer membro do público, por exemplo, uma praça, um centro comercial, uma rua, um mercado, uma estação de comboios ou uma biblioteca pública.

[276] O GT29 avança com o exemplo de um hospital geral que mantenha registos médicos dos doentes ou de um investigador privado que mantenha informações acerca dos autores das infrações.

população que necessitem de proteção especial (pessoas com doenças mentais, requerentes de asilo, idosos, doentes, etc.) e todos os casos em que possa ser identificado um desequilíbrio na relação entre a posição do titular dos dados e o responsável pelo tratamento;

8. Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais, tais como combinar a utilização da impressão digital e do reconhecimento facial para melhorar o controlo do acesso físico, etc. O RGPD deixa claro (artigo 35.º, n.º 1, e Considerandos 89 e 91) que a utilização de uma nova tecnologia, definida em "conformidade com o nível de conhecimentos tecnológicos alcançado" (considerando 91), pode desencadear a necessidade de realização de uma AIPD. Isto acontece porque a utilização dessa tecnologia pode envolver novas formas de recolha e utilização de dados, possivelmente com elevado risco para os direitos e as liberdades dos indivíduos. Na verdade, as consequências pessoais e sociais da implantação de uma nova tecnologia podem ser desconhecidas. Uma AIPD ajudará o responsável pelo tratamento de dados a compreender e dar resposta a esses riscos. Por exemplo, algumas aplicações da «Internet das Coisas» podem ter um impacto significativo na vida quotidiana e na privacidade dos indivíduos e, como tal, exigem a realização de uma AIPD;
9. Quando o próprio tratamento impede os titulares dos dados "de exercer um direito ou de utilizar um serviço ou um contrato" (artigo 22.º e Considerando 91). Estão incluídas operações de tratamento destinadas a autorizar, alterar ou recusar o acesso dos titulares dos dados a um serviço ou que estes celebrem um contrato[277].

É importante ter em consideração que, na maioria dos casos, o responsável pelo tratamento poderá considerar que um tratamento que satisfaça pelo menos dois dos critérios acima descritos exige a realização de uma AIPD. Segundo o GT29 quanto mais critérios se aplicarem mais provável é que o processamento contenha um risco elevado para os direitos e as liberdades dos titulares dos dados e, por conseguinte, de necessitar de uma AIPD, independentemente das medidas que o responsável pelo tratamento pretender adotar.

No entanto, em alguns casos, um responsável pelo tratamento de dados pode considerar que um tratamento que satisfaça apenas um dos critérios exige a realização de uma AIPD. Daí que o GT29, nas suas Orientações, tenha concebido diversos exemplos práticos que ilustram a forma como os critérios devem ser utilizados para avaliar se uma operação de tratamento específica exige ou não uma AIPD[278].

Por sua vez, é igualmente admissível que uma operação de tratamento pode integrar algum ou alguns dos critérios supramencionados e continuar a ser considerada pelo responsável pelo tratamento como uma operação que não é "suscetível de implicar um elevado risco". Contudo, nestes casos, o responsável pelo tratamento deve

[277] O GT29 dá como o exemplo um banco que faz um controlo seletivo dos seus clientes a partir de uma base de dados de referências de crédito bancário com vista a decidir se lhes concede ou não um empréstimo.

[278] GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, Op. Cit. p. 13-14.

justificar e documentar as razões que o levam a não realizar uma AIPD e incluir/registar os pontos de vista do encarregado da proteção de dados.

Importa ter em conta que, como decorrência do princípio da responsabilidade, cada responsável pelo tratamento de dados "conserva um registo de todas as atividades de tratamento sob a sua responsabilidade", onde constam, entre outros, as finalidades do tratamento dos dados, a descrição das categorias de titulares de dados e das categorias de dados pessoais e "[s]e possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.º, n.º 1" (cfr. artigo 30.º, n.º 1) e deve avaliar a probabilidade de ser suscetível de implicar um elevado risco, mesmo que acabem por decidir não realizar uma AIPD.

A este propósito, os critérios acima expostos, servem ainda para auxiliar as autoridades de controlo a elaborar e comunicar a lista das operações de tratamento sujeitas ao requisito de AIPD junto do Comité Europeu para a Proteção de Dados (CEPD) nos termos do previsto no n.º 4 do artigo 35.º. No caso português, nos termos da alínea k) do n.º 1 do artigo 57.º e em cumprimento do referido n.º 4 do artigo 35.º, a CNPD aprovou o Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados[279]. A lista contida neste Regulamento teve igualmente em consideração as recomendações incluídas no Parecer n.º 18/2018 do CEPD[280] que, por sua vez, procurou aplicar os adequados mecanismos de controlo de coerência ao projeto de lista e às operações de tratamento aí elencadas. Assim, a CNPD aprovou a seguinte lista de tratamentos de dados pessoais sujeitos a AIPD, que acrescem aos previstos no n.º 3 do artigo 35.º:

1. Tratamento de informação decorrente da utilização de dispositivos eletrónicos que transmitam, por redes de comunicação, dados pessoais relativos à saúde[281];
2. Interconexão de dados pessoais[282] ou tratamento que relacione dados pessoais previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal[283];

---

[279] Publicado no Diário da República, 2.ª série, N.º 231, de 30 de novembro de 2018.

[280] CEPD – Parecer n.º 18/2018 sobre o projeto de lista da autoridade de controlo competente de Portugal respeitante às operações de tratamento de dados pessoais sujeitas a avaliação de impacto sobre a proteção de dados (artigo 35.º, n.º 4, do RGPD). Adotado em 25 de setembro de 2018. [Em Linha]. Disponível em https://edpb.europa.eu/sites/default/files/files/file1/edps-2018-00017-00-14_pt.pdf.

[281] Por exemplo, peças de vestuário equipadas com *chip* que transmita dados de saúde acerca do seu portador, *apps* de desporto ou de saúde, etc.

[282] Tanto no RGPD, concretamente, no cardápio das definições legais estabelecidas no seu artigo 4.º, como na própria Lei n.º 58/2019, de 08 de Agosto, a chamada Lei de Execução, não consta o conceito de "interconexão de dados pessoais". Para o encontrar temos que recorrer à definição prevista na al. i) do artigo 3.º da Lei n.º 67/98, de 26/10 (LPDP), entretanto revogada pela atual Lei n.º 58/2019, de 08 de Agosto, que previa o seguinte: "Para efeitos da presente lei, entende-se por: (…) i) 'Interconexão de dados': forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade". A única referência à interconexão no RGPD aparece na própria definição de "Tratamento", logo no número 2 do artigo 4.º, em que se dispõe o seguinte: "Para efeitos do presente regulamento, entende-se por: (…) 2) "Tratamento", uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição".

[283] Segundo o GT29, nas suas Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, para além das mencionadas disposições do RGPD, algumas categorias de dados podem ser consideradas como

3. Tratamento de dados pessoais previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal com base em recolha indireta dos mesmos, quando não seja possível ou exequível assegurar o direito de informação nos termos da alínea b) do n.º 5 do artigo 14.º do RGPD;
4. Tratamento de dados pessoais que implique ou consista na criação de perfis em grande escala;
5. Tratamento de dados pessoais que permita rastrear a localização ou os comportamentos dos respetivos titulares (por exemplo, trabalhadores, clientes ou apenas transeuntes), que tenha como efeito a avaliação ou classificação destes, exceto quando o tratamento seja indispensável para a prestação de serviços requeridos especificamente pelos mesmos[284];
6. Tratamento dos dados previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou ainda dos dados de natureza altamente pessoal para finalidade de arquivo de interesse público, investigação científica e histórica ou fins estatísticos, com exceção dos tratamentos previstos e regulados por lei que apresente garantias adequadas dos direitos dos titulares;
7. Tratamento de dados biométricos para identificação inequívoca dos seus titulares, quando estes sejam pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados;
8. Tratamento de dados genéticos de pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados;
9. Tratamento de dados pessoais previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal com utilização de novas tecnologias ou nova utilização de tecnologias já existentes.

2.6 Casos em que não é obrigatória

O GT29 considera que uma AIPD não é obrigatória nos casos seguintes:

- quando o tratamento não for "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (artigo 35.º, n.º 1);

- quando a natureza, o âmbito, o contexto e as finalidades do tratamento forem muito semelhantes ao tratamento em relação ao qual tenha sido realizada uma AIPD. Nestes casos, podem ser utilizados os resultados da AIPD realizada para o tratamento semelhante (artigo 35.º, n.º 1);

---

categorias que aumentam os possíveis riscos para os direitos e as liberdades dos indivíduos. Estes dados pessoais são considerados sensíveis (na aceção comum deste termo) porque estão associados a atividades privadas e familiares – são "dados de natureza altamente pessoal" – e incluem, entre outros, as comunicações eletrónicas pessoais, os dados de localização, os dados financeiros, os documentos pessoais, os diários, as notas em dispositivos eletrónicos de leitura, os calendários virtuais com as consultas médicas ou os locais visitados, etc.

[284] Estes tratamentos de dados pessoais são cada vez mais utilizados em diversos domínios, tais como, serviços de logística de entregas de bens de consumo ao domicílio ou plataformas eletrónicas de transporte individual e remunerado de passageiros em veículos descaracterizados. No setor dos transportes, os sindicatos alegam falta de transparência e exigem a regulamentação do uso da Inteligência Artificial e dos algoritmos nas relações de trabalho (cfr. suplemento de economia do Expresso de 02.07.2021). No desporto tem assumido polémica o chamado "Project Red Card" relativo à obtenção de dados pessoais dos jogadores por parte das empresas de apostas, e até mesmo de videojogos, durante as sessões de treino, nos jogos de futebol e nas transmissões televisivas, para além de outras formas que permitem recolher os dados dos atletas, os quais são tratados para fins estatísticos, de classificação e previsão, na maior parte dos casos, sem qualquer controlo por parte dos titulares dos dados – Crf. SILVA, Hugo Tavares – A quem pertencem os dados? Primeiro Caderno. Expresso. Lisboa. (06 nov. 2021). P. 36.

- quando as operações de tratamento tiverem sido previamente controladas por uma autoridade de controlo antes de maio de 2018 em condições específicas que não se tenham alterado;

- quando uma operação de tratamento, nos termos do artigo 6.º, n.º 1, alíneas c) ou e), tiver um fundamento jurídico no direito da UE ou de um Estado-Membro, em que o direito regule a operação de tratamento específica e em que a AIPD já tenha sido realizada como parte da adoção desse fundamento jurídico (artigo 35.º, n.º 10), salvo se o Estado-Membro considerar necessário proceder a essa avaliação antes das atividades de tratamento;

- quando o tratamento estiver incluído na lista opcional (definida pela autoridade de controlo) de operações de tratamento para as quais não é obrigatória uma AIPD (artigo 35.º, n.º 5).

No que respeita às operações de tratamento já existentes, as AIPD são obrigatórias nalgumas circunstâncias, desde logo, são aplicáveis às operações de tratamento existentes suscetíveis de implicar um elevado risco para os direitos e as liberdades das pessoas singulares e em relação às quais não tenha havido alteração dos riscos, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

No entanto, não é necessário realizar uma AIPD para operações de tratamento que tenham sido previamente controladas por uma autoridade de controlo ou pelo encarregado da proteção de dados, em conformidade com o artigo 20.º da D 95/46, e que sejam realizadas sem alterações desde o controlo prévio anterior. Conforme se esclarece no Considerando 171, "as decisões da Comissão que tenham sido adotadas e as autorizações que tenham emitidas pelas autoridades de controlo com base na D 95/46, permanecem em vigor até ao momento em que sejam alteradas, substituídas ou revogadas".

Por sua vez, qualquer tratamento de dados cujas condições de aplicação (âmbito, finalidade, recolha de dados pessoais, identidade dos responsáveis pelo tratamento dos dados ou dos destinatários, período de retenção dos dados, medidas técnicas e organizativas, etc.) tenham mudado desde o controlo prévio realizado pela autoridade de controlo ou pelo encarregado da proteção dos dados e que sejam suscetíveis de implicar um elevado risco devem ser sujeitas a uma AIPD.

Igualmente, pode ser obrigatório realizar uma AIPD após uma alteração dos riscos decorrentes das operações de tratamento, por exemplo, porque se começou a utilizar uma nova tecnologia ou porque os dados pessoais passaram a ser utilizados para uma finalidade diferente.

Por último, o GT29 recomenda, como boa prática, que a AIPD seja continuamente revista e regularmente reavaliada. Nesse sentido, mesmo que não seja obrigatória a realização de uma AIPD em 25 de maio de 2018, será necessário, na altura adequada, que o responsável pelo tratamento realize essa AIPD como parte das suas obrigações gerais em matéria de responsabilização.

2.7 Abordagem baseada no risco

O RGPD refere-se ao termo "risco" setenta e três vezes ao longo do texto e, especificamente, nos n.ºs 1 e 4 do artigo 24.º, na al. g) do n.º 2 do artigo 23.º, nos artigos 25.º, 27.º, 30.º, 32.º, 33.º, 34.º, 35.º, 36.º, 39.º, 49.º, entre outros.

A "abordagem baseada no risco" é desenvolvida na "*Statement on the role of a risk-based approach in data protection legal frameworks WP218*" (doravante a Declaração WP218) e não é um conceito novo no quaro legal da proteção de dados. No entanto, como bem se refere na referida Declaração WP218[285], a "abordagem baseada no risco" adquiriu maior relevância nas discussões no Parlamento Europeu e no Conselho sobre a proposta de RGPD, acabando por se constituir como um elemento central do próprio princípio de responsabilidade (n.º 2 do artigo 5.º e artigo 24.º). Para além da obrigação de caução e da obrigação de realizar uma avaliação de impacto, a abordagem baseada no risco foi estendida e refletida em outras medidas de implementação, como o princípio da proteção de dados desde a conceção e por defeito (artigo 25.º), a obrigação de documentação (artigo 30.º) e o uso de certificação e códigos de conduta (artigos 40.º e 42.º).

O RGPD estabelece a obrigação de gerir o risco que um tratamento implica para os direitos e liberdades das pessoas singulares. Este risco surge tanto da própria existência do tratamento, bem como das dimensões técnicas e organizacionais do mesmo. O risco surge tanto do tratamento automatizado dos dados como do seu tratamento manual, dos elementos humanos e dos recursos envolvidos. O risco decorre das finalidades do tratamento e da sua natureza, assim como do âmbito e do contexto em que se desenvolve (artigo 25.º).

O RGPD não estabelece um critério prático-metodológico para a gestão dos riscos. Nesse aspeto, o RGPD deixa liberdade para que essa gestão do risco para os direitos e liberdades seja, ou possa ser, integrada com os restantes recursos de gestão do risco, das políticas e da governança da organização.

Em geral, o RGPD não faz sequer qualquer exigência explícita de alguma formalidade quanto à execução da gestão de riscos, sem prejuízo das obrigações de "responsabilidade" já acima mencionadas. No entanto, para tratamentos que envolvem elevado risco, o RGPD estabelece requisitos mínimos que a sua gestão deve ter. Estes derivam, especialmente, das obrigações estabelecidas nos artigos 35.º relativa à "Avaliação de Impacto da Proteção de Dados" e no artigo 36.º relativa à "Consulta prévia".

Nesse sentido, e como acima se expôs, o GT29 (atual Comité Europeu de Proteção de Dados) desenvolveu as "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679". Nas referidas Orientações um "risco" é um cenário que descreve um acontecimento e as respetivas consequências, estimado em termos de gravidade e probabilidade. Por sua vez, a "gestão do risco" é definida como as atividades coordenadas que visam direcionar e controlar uma organização no que toca ao risco[286].

---

[285] GT29 - Statement on the role of a risk-based approach in data protection legal frameworks (WP218), Op. Cit. p. 2.

[286] GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, Op. Cit. p. 7.

Como bem se refere nas referidas Orientações, o risco para os direitos e liberdades dos titulares dos dados "diz sobretudo respeito aos direitos de proteção dos dados e privacidade, mas também envolve outros direitos fundamentais como a liberdade de expressão, a liberdade de pensamento, a liberdade de circulação, a proibição de discriminação, o direito à liberdade, consciência e religião"[287].

O Considerando 75 desenvolve o conceito de risco para os direitos e liberdades como qualquer efeito ou consequência não desejado ou imprevisto sobre as pessoas singulares ou não previsto no próprio tratamento de dados pessoais, capazes de gerar danos ou prejuízos nos seus direitos e liberdades, especificando, entre outros: danos físicos, materiais ou imateriais, problemas de discriminação, roubo de identidade ou fraude, perda financeira, dano à reputação, perda de confidencialidade de dados sujeitos a sigilo profissional, inversão não autorizada de pseudonimização, danos económicos ou sociais, privação dos titulares dos dados dos seus direitos e liberdades ou do exercício do controlo sobre os respetivos dados pessoais.

Além disso, na Declaração WP218 elucida-se que, na abordagem baseada no risco, a proteção desses direitos deve ser realizada avaliando tanto o impacto que o tratamento em questão tem na pessoa afetada, bem como o impacto social geral que pode causar. Neste último caso, apresenta-se como exemplo concreto a eventual perda da confiança social (quando no ponto 11 se *refere "The risk-based approach …, assessed on a very wide scale ranging from an impact on the person concerned by the processing in question to a general societal impact (e.g. loss of social trust)."*

Portanto, não é apenas necessário gerir os riscos para o titular dos dados que estão a ser tratados, mas os de todos aqueles indivíduos afetados ou de grupos afetados pelo tratamento, uma vez que, não raras vezes, o objetivo de um tratamento não é outro senão o de classificar as pessoas num grupo específico. Pese embora a dimensão usual seja o indivíduo, muitas vezes as decisões que são tomadas pelo responsável pelo tratamento podem afetar os direitos de grupos de pessoas.

Em suma, o foco da gestão do risco no RGPD é a proteção da pessoa, na sua dimensão individual e social, enquanto titular dos dados pessoais ou afetada pelo seu tratamento. Embora tenha uma relação colateral, a gestão de riscos para os direitos e liberdades não visa proteger os interesses do responsável ou responsáveis pelo tratamento em relação com este, por exemplo, quanto à continuidade do tratamento, sua eficácia ou sua eficiência, ou conformidade regulatória ou em relação às possíveis atividades comerciais do próprio responsável.

Todas as atividades de tratamento de dados pessoais envolvem um risco para as pessoas cujos dados são tratados e, em particular, para os seus direitos e liberdades. Mesmo naqueles casos em que o responsável pelo tratamento, seja pelo tipo de dados ou devido ao tipo de atividade da organização, poderia assumir a existência de um risco escasso para os titulares dos dados ou mesmo a inexistência de risco.

Neste sentido, o GT29 esclarece a importância de realizar a gestão do risco nos tratamentos mesmo quando estes não são de elevado risco: " (…) o simples facto de as condições que conduzem à obrigação de realizar uma AIPD não terem sido satisfeitas não diminui a obrigação geral que os responsáveis pelo tratamento têm de aplicar

[287] Idem – Ibidem.

medidas que visem gerir adequadamente os riscos para os direitos e as liberdades dos titulares dos dados"[288].

Pelo que, o conceito de "risco zero" não existe quando falamos de gestão do risco, em particular, quando falamos sobre os riscos que podem decorrer da realização de tratamentos de dados pessoais. Haverá sempre um risco inicial inerente ou implícito (risco bruto) em qualquer tratamento e, uma vez aplicadas as medidas e garantias para a sua minimização, ainda haverá um risco residual.

A Declaração WP218 clarifica que a abordagem baseada no risco deve ser um processo escalável e adaptável à situação específica de cada tratamento. A abordagem baseada no risco deve ser proporcional e o desempenho do processo de gestão do risco para os direitos e liberdades deve ser guiado por princípios de eficácia e eficiência. A complexidade do processo de gestão de risco tem de ser ajustada, não ao tamanho da organização, à disponibilidade de recursos ou à sua especialidade ou setor, mas ao possível impacto da atividade de tratamento sobre os titulares dos dados. Se uma entidade pretende realizar um tratamento e não tem a capacidade para fazer a gestão do risco necessária, será forçada a procurar algum tipo de ajuda, como recorrer a consultoria externa, de forma a realizá-la no modo apropriado.

A gestão de risco deve ser abordada como um processo transversal a toda a organização e ligá-la ao resto dos processos existentes a fim de alcançar uma estrutura de gestão de risco global, abrangente, eficaz e eficiente que abrange a organização como um todo e em todas as suas dimensões. O compromisso adotado pelos responsáveis pela organização na referida gestão é um fator chave para o sucesso.

Por último, mas não menos importante, a Declaração WP218 evidencia que a abordagem baseada no risco deve ir mais além de que uma mera abordagem apenas para reagir a um dano causado ao titular dos dados (reativa).

A gestão do risco não deve ser reduzida à mera gestão das consequências que ocorreram no titular dos dados como sucede, por exemplo, no caso de violação de dados pessoais. A gestão de riscos deve incluir uma abordagem preventiva (pró-ativa). Nesse sentido, ao determinar os fatores de risco a serem geridos, é necessário levar em consideração o contexto presente e os potenciais contextos futuros. A gestão de riscos requer uma avaliação de longo prazo, especialmente naqueles cenários cujo impacto pode resultar num prejuízo muito elevado para os titulares dos dados ou para a sociedade.

2.8 Metodologia e conteúdo

O RGPD estabelece o conteúdo mínimo que a AIPD deve incluir, bem como o facto de se dever ter em conta, na sua realização, o cumprimento dos códigos de conduta pelos responsáveis ou pelos subcontratantes (n.º 8 do artigo 35.º do RGPD). A avaliação, nos termos do n.º 7 do artigo 35.º, deve incluir pelo menos os seguintes aspetos:

a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;

b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;

[288] Idem – Ibidem.

c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos; e

d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

O RGPD, como acima se disse, permite que o responsável pelo tratamento determine como irá realizar a AIPD, tendo em conta a sua organização, de forma que possa ser adaptada às operações de tratamento e processos de negócio. Neste sentido, uma microempresa ou uma PME poderá conceber uma metodologia de acordo com as suas operações de tratamento. A este propósito, o GT29 incentivou o desenvolvimento de quadros específicos para cada setor, podendo tirar partido de conhecimentos setoriais específicos, o que quer dizer que a AIPD pode responder às especificidades de determinado tipo de operação de tratamento (p. ex. determinados tipos de dados, ativos empresariais, impactos potenciais, ameaças, medidas). Equivale isto a dizer que a AIPD pode abordar os problemas que surgem num determinado setor económico ou quando se utilizam determinadas tecnologias ou quando se realizam determinados tipos de operações de tratamento[289].

No entanto, o GT29 deixou claro que a AIPD, ao abrigo do RGPD, é um instrumento que visa a análise e a gestão dos riscos para os direitos dos titulares dos dados, e, como tal, avalia-os na perspetiva destes últimos, como acontece em determinados domínios (p. ex. segurança societal). Em contrapartida, a gestão dos riscos noutros domínios (p. ex. segurança da informação) centra-se na organização. Daí que o Considerando 90 enuncia vários elementos da AIPD que se sobrepõem a elementos bem definidos da gestão do risco (p. ex. ISO 31000). Em matéria de gestão dos riscos, uma AIPD destina-se a "gerir os riscos" para os direitos e as liberdades das pessoas singulares, utilizando os seguintes processos:

- estabelecendo o contexto: "tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco";

- avaliando os riscos: "avaliar a probabilidade ou gravidade particulares do elevado risco";

- dando resposta aos riscos: "atenuar esse risco" e "assegurar a proteção dos dados pessoais" e "comprovar a observância do RGPD".

O RGPD dá aos responsáveis pelo tratamento de dados a flexibilidade necessária para determinar a estrutura e a forma precisas da AIPD com vista a que esta se encaixe nas práticas de trabalho existentes. Existem vários processos diferentes na UE e a nível mundial[290] que têm em conta os elementos descritos no Considerando 90.

---

[289] Idem – Ibidem. P. 20.

[290] A este propósito existem vários modelos provenientes das diferentes autoridades europeias de proteção de dados, entre outras, a francesa CNIL (Commission Nationale de l'Informatique et des Libertés), a espanhola AEPD (Agencia Española de Protección de Datos) ou a britânica ICO (Information Commissioner´s Office) – Cfr. GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, Op. Cit. p. 24 (Anexo 1: Exemplos de quadros existentes na UE em matéria de AIPD). Existem ainda algumas Normas ISO relativas à segurança da informação que podem conter algumas orientações válidas para adaptação à organização no sentido de implementar medidas que ajudem a proteger os dados pessoais. Entre elas,

Contudo, seja qual for a sua forma, uma AIPD deve avaliar genuinamente os riscos, permitindo assim que os responsáveis pelo tratamento tomem medidas para dar resposta a esses riscos. A este respeito, os responsáveis pelo tratamento não devem considerar a AIPD como um mero exercício formal e instantâneo apenas para tentar demostrar conformidade junto da autoridade de controlo, mas como um instrumento ou um processo contínuo de genuína avaliação do risco.

Independentemente da metodologia utilizada, o GT29 estabeleceu, de acordo com as fases que a AIPD deve incluir, alguns critérios comuns que o modelo ou método escolhido pelo responsável pelo tratamento deve ter em conta e que abaixo se condensa.

Fig. 1 – Ilustra o processo iterativo genérico para a elaboração de uma AIPD.
Fonte GT29 17/PT WP 248 rev.01, p. 19.

a) Análise preliminar

Nesta fase, deve ser averiguado se há lugar à realização de uma AIPD. Para o efeito, devem ser consultadas previamente as eventuais listas emitidas pela autoridade de controlo competente, de forma a verificar se o tratamento em causa pode enquadrar-se em alguma das hipóteses que foram estabelecidas, quer na lista dos tratamentos que devem ser objeto de AIPD - no caso português, os constantes do já citado Regulamento n.º 1/2018 aprovado pela CNPD - ou na dos que não devem ser objeto de AIPD.

Em segundo lugar, deve ser analisado se o tratamento pode ser incluído em algum dos casos de avaliação obrigatória indicados no n.º 3 do artigo 35.º ou na exclusão prevista no n.º 10 do mesmo artigo.

destaca-se a Norma ISO 27701 que é a norma para implementar sistemas de gestão da informação relativa a pessoas. Esta Norma conjuga a ISO 27001 relativa à implementação de sistemas de gestão de segurança de informação com a ISO 27002 relativa aos controlos a efetivar para garantir que o sistema de gestão de segurança da informação está a cumprir com o que é idealizado ou desenhado.

Em terceiro lugar, se o tratamento não tiver sido reconduzido às aludidas listas ou a qualquer um dos casos do n.º 3 do artigo 35.º, deve então ser feita uma classificação do tratamento com base no risco que representa para os direitos e liberdades dos titulares dos dados. Para isso, podem ser utilizados os critérios estabelecidos pelo GT29 nas já citadas Orientações relativas à AIPD. De referir que, nesta fase, estamos apenas concentrados no impacto dos possíveis riscos para os direitos e liberdades e não ainda na probabilidade de ocorrência do evento que materializa a situação de risco. Por esta razão, todos os critérios utilizados para realizar esta primeira análise incidem sobre os danos que os titulares dos dados podem sofrer ou sobre os tratamentos que têm potencial para os causar.

Importa ainda ter em consideração que, para realizar esta análise e respetivo enquadramento, será sempre necessário fazer uma descrição inicial do tratamento que permita a aplicação dos referidos critérios.

Finalmente, somente se o tratamento for considerado de elevado risco é que a AIPD deve ser realizada.

b) Descrição sistemática das operações de tratamento[291]

Nesta fase é necessário realizar uma descrição sistemática das operações de tratamento (n.º 7 do artigo 37.º), que deve incluir os aspetos seguintes:

- a natureza, o âmbito, o contexto e as finalidades do tratamento (Considerando 90);
- os dados pessoais, os destinatários e o período de conservação dos dados;
- a descrição funcional do tratamento (prevendo o funcionamento do "ciclo de vida dos dados");
- os ativos que suportam os dados (p. ex., *hardware*, *software*, redes, pessoas, etc);
- a existência de algum código de conduta a que o responsável pelo tratamento e/ou o subcontratante estejam vinculados (n.º 8 do artigo 35.º). Neste caso, teria que se averiguar eventuais regras adicionais que pudessem determinar uma metodologia própria para a realização de AIPD.

c) Avaliação da necessidade e da proporcionalidade

Outra fase que a AIPD deve ter é a avaliação da necessidade e da proporcionalidade do tratamento (al. b) do n.º 7 do artigo 35.º). Tal implica que a finalidade do tratamento terá que ser analisada para se poder determinar se o tratamento é realmente necessário e proporcional. O que esta avaliação exige é a verificação do cumprimento dos princípios relativos ao tratamento dos dados que já acima tivemos oportunidade de expor e, principalmente, a observância dos princípios da minimização de dados e da licitude. Relativamente a este último, deverá ser averiguada a adequação do fundamento de licitude escolhido para o tratamento que, caso seja o interesse legítimo, conforme especificado na al. a) do n.º 7 d o artigo 35.º, este deve ser descrito e, consequentemente, feita a ponderação entre o interesse legítimo do responsável pelo tratamento e os interesses ou direitos e liberdades fundamentais dos titulares dos dados.

[291] Cfr. GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, Op. Cit. p. 26. [Anexo 2 — Critérios para uma AIPD aceitável].

Igualmente, deve ser avaliada a proporcionalidade da operação de tratamento, o que nos remete para o princípio da proporcionalidade amplamente refletido na jurisprudência[292] e na doutrina e que se desdobra, analiticamente, em três subprincípios: o princípio da adequação (que pressupõe que o tratamento é adequado ao objetivo perseguido), o princípio da exigibilidade ou necessidade (que implica que o tratamento é necessário, no sentido de que não há outra medida alternativa menos onerosa para o titular dos dados); e, por fim, o princípio da justa medida ou proporcionalidade em sentido estrito (segundo o qual o tratamento será ponderado e equilibrado, não podendo adotar-se medidas excessivas, desproporcionadas para alcançar os fins pretendidos).

Em síntese, o que está em causa é avaliar se o tratamento é necessário e proporcional à finalidade pretendida[293]. Pelo que, se o resultado da avaliação for negativo, o tratamento deve ser reformulado ou então prescindida a sua realização.

d) Identificação das medidas previstas para demonstrar a conformidade[294]

De acordo com o GT29, na identificação destas medidas, deve-se ter em consideração aquelas que contribuem para a proporcionalidade e a necessidade do tratamento tendo por base:

- Finalidades determinadas, explícitas e legítimas (al. b) do n.º 1 do artigo 5.º);
- Licitude do tratamento (artigo 6.º);
- Dados adequados, pertinentes e limitados ao necessário (al. c) do n.º 1 do artigo 5.º);
- Limitação da conservação (al. e) do n.º 1 do artigo 5.º).

Igualmente devem ser consideradas as medidas que contribuem para assegurar os direitos dos titulares dos dados, a saber:

- Informação (artigos 12.º, 13.º e 14.º);
- Acesso e portabilidade (artigos 15.º e 20.º);
- Retificação e apagamento (artigos 16.º, 17.º e 19.º);
- Oposição e limitação do tratamento (artigos 18.º, 19.º e 21.º);
- Relação com os subcontratantes (artigo 28.º);
- Garantias relativas às transferências internacionais (Capítulo V do RGPD);
- Consulta prévia (artigo 36.º).

e) Avaliação dos riscos para os direitos e liberdades[295]

Nesta fase deverá ser realizada a avaliação dos riscos do tratamento para os direitos e liberdades dos titulares dos dados (al. c) do n.º 7 do artigo 35.º).

---

[292] ALMEIDA, Luís Nunes de Relat. - Acórdão do Tribunal Constitucional n.º 634/93 – Processo nº 94/92. [Em linha]. [Consult. 26 abr 2022]. Disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19930634.html.

[293] A título de exemplo, no contexto laboral, para fins de controlo do desempenho do trabalhador, de prova de cumprimento de contrato ou de legislação rodoviária e de utilização de viatura para fins privados, Lurdes Dias Alves salienta que: "No uso de sistemas de geolocalização de telemóveis, tablets ou computadores portáteis, as finalidades visadas são geralmente a proteção do bem em si, considera-se excessivo e desproporcional a utilização deste tipo de tecnologia, pelo que a sua utilização é proibida". Cfr. ALVES, Lurdes Dias – Proteção de Dados Pessoais no Contexto Laboral. Coimbra: Edições Almedina, novembro de 2020. ISBN978-972-40-8581-4. P. 37.

[294] Cfr. GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, Op. Cit. p. 26. [Anexo 2 — Critérios para uma AIPD aceitável].

[295] Idem – Ibidem.

Na aludida avaliação devemos ter em consideração a origem, a natureza, a particularidade e a gravidade dos riscos (Considerando 84) ou, mais especificamente, cada risco (acesso ilegítimo, modificação indesejada, desaparecimento de dados) da perspetiva dos titulares dos dados. Para isso, devemos garantir que:

- as fontes de risco são tidas em conta (considerando 90);
- os potenciais impactos nos direitos e nas liberdades dos titulares dos dados são identificados na eventualidade de acesso ilegítimo, modificação indesejada e desaparecimento de dados, entre outros;
- as ameaças que possam conduzir a acesso ilegítimo, modificação indesejada e desaparecimento de dados são identificadas;
- a probabilidade e a gravidade são estimadas (considerando 90);
- as medidas previstas para fazer face a esses riscos são determinadas (al. d) do n.º 7 do artigo 35.º e Considerando 90);

Nessa avaliação, como já explanamos na parte dedicada à abordagem baseada no rico[296], deve-se ter em consideração o risco inerente (bruto), que é aquele que existe antes de avaliar as medidas previstas para mitigá-lo. Posteriormente, será incorporada a avaliação dessas medidas previstas para que se obtenha o risco residual.

f) Medidas para enfrentar os riscos

Avaliados os riscos, será então necessário identificar medidas adicionais às medidas já previstas que podem ser adotadas para mitigar o risco residual, caso este ainda se encontre num nível elevado (al. d) do n.º 7 do artigo 35.º e considerando 90). Se não for possível adotar medidas adicionais ou se as medidas adicionais adotadas não mitigarem o elevado risco residual, então há lugar à obrigação de consultar a autoridade de controlo.

g) Documentação

É essencial que, por força do princípio da responsabilidade, todo o processo de avaliação seja documentado, devendo a AIPD refletir os resultados do processo e suas conclusões. Importa ter em conta que a AIPD completa deve ser comunicada à autoridade de controlo em caso de consulta prévia ou se tal for solicitado pela autoridade de proteção de dados.

O GT29 recomenda que os responsáveis pelo tratamento devem considerar, pelo menos, a publicação parcial da AIPD, mediante, por exemplo, um resumo, uma conclusão ou uma mera declaração de realização. Não será necessário publicar a totalidade da AIPD, especialmente, quando nela constem informações específicas sobre riscos de segurança para o responsável pelo tratamento de dados ou segredos comerciais ou informações comercialmente sensíveis. A publicação parcial serve para aumentar a confiança nas operações de tratamento do responsável pelo tratamento e para demonstrar responsabilidade e transparência[297].

---

[296] Cfr. Ponto 3.7 do presente Relatório.

[297] GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, Op. Cit. p. 21.

h) Controlo ou revisão

O RGPD veio estabelecer que, se necessário, o responsável pelo tratamento deve proceder a um controlo para avaliar a conformidade do tratamento com a avaliação de impacto (n.º 11 do artigo 35.º). Segundo A. Barreto Menezes Cordeiro, a remissão para o conceito amplo de necessidade dá ao responsável pelo tratamento uma ampla margem de decisão em seu favor, pelo que o legislador da U.E., em consideração dos interesses dos titulares dos dados, ilustrou a necessidade de revisão (obrigatória) "quando haja uma alteração dos riscos que as operações de tratamento representam"[298].

Fora deste caso, concede-se ao responsável pelo tratamento a determinação da periodicidade do referido controlo ou revisão, sendo certo que a atualização da AIPD ao longo do ciclo de vida do projeto garantirá que a proteção dos dados e a privacidade serão consideradas e incentivará a criação de soluções que promovam a conformidade.

i) Audição dos interessados

Por último, o RGPD vem prever que o responsável pelo tratamento, em certos casos, que o n.º 9 do artigo 35.º não especifica, solicita a opinião dos titulares de dados ou seus representantes sobre o tratamento. Esta norma parece colocar na disponibilidade do responsável pelo tratamento a decisão de audição dos interessados. Trata-se, porém, de uma obrigação que recai sobre o responsável pelo tratamento, sempre que seja adequado ouvir aqueles interessados: o que implica que caso assim não o entenda, deverá o referido responsável justificá-lo documentando-o[299].

O GT29 sugere alguns meios para a audição dos titulares de dados ou seus representantes, nomeadamente, mediante um estudo genérico relacionado com a finalidade e os meios da operação de tratamento, uma questão colocada aos representantes do pessoal ou através de inquéritos. Pese embora existir flexibilidade nos meios a usar para ouvir as opiniões dos interessados, o consentimento não é a forma mais idónea de o fazer. O responsável pelo tratamento deve justificar, documentando-as, as razões que o levaram a prosseguir o tratamento, se a opinião dos titulares for diferente[300].

2.9. Intervenção do Encarregado de Proteção de Dados

Nos termos do n.º 1 do artigo 35.º, cabe ao responsável pelo tratamento, e não ao EPD, proceder, quando necessário, a uma avaliação de impacto sobre a proteção de dados (AIPD). Todavia, o EPD pode desempenhar um papel muito importante e útil, prestando assistência ao responsável pelo tratamento.

Aplicando o princípio da proteção de dados desde a conceção, o n.º 2 do artigo 35.º dispõe expressamente que, ao efetuar uma AIPD, o responsável pelo tratamento deve "solicita[r] o parecer" do EPD. Pelo que, o referido parecer é obrigatório, a pedido do responsável pelo tratamento, se o EPD tiver sido designado.

---

298 CORDEIRO, A. Barreto Menezes – Comentário, Op. Cit. p. 284.

299 Idem – Inidem.

300 GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, Op. Cit. p. 17.

Por sua vez, a al. c) do n.º 1 do artigo 39.º determina que o EPD "presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35.º".

Concretizando o papel do EPD no âmbito da AIPD, o GT29 recomenda que o responsável pelo tratamento solicite o parecer do EPD sobre as seguintes questões, entre outras:

- se deve ou não efetuar uma AIPD;
- qual a metodologia a seguir na realização de uma AIPD;
- se deve realizar a AIPD internamente ou externamente;
- quais as salvaguardas (incluindo medidas técnicas e organizativas) a aplicar no sentido de atenuar os eventuais riscos para os direitos e interesses dos titulares de dados;
- se a avaliação de impacto sobre a proteção de dados foi ou não corretamente efetuada e se as suas conclusões (se o tratamento deve ou não ser realizado e quais as salvaguardas a aplicar) estão em conformidade com o RGPD[301].

Se o responsável pelo tratamento discordar do parecer emitido pelo EPD, a documentação da AIPD deve justificar especificamente, por escrito, os motivos pelos quais o parecer não foi tido em conta. Importa aqui lembrar, enquanto decorrência princípio da responsabilidade, a obrigação que recai sobre o responsável pelo tratamento de aplicar as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o RGPD, nos termos do n.º 1 do artigo 24.º.

O GT29 recomenda, além disso, que o responsável pelo tratamento indique claramente, por exemplo, no contrato com o EPD, bem como nas informações prestadas aos trabalhadores e aos quadros de gestão (e a outras partes interessadas, se for caso disso), as tarefas específicas do EPD e o respetivo âmbito de aplicação, nomeadamente no que diz respeito à realização da AIPD[302].

2.9. Consulta à Autoridade de Controlo

Como foi mencionado anteriormente, a autoridade de controlo deve ser consultada quando os riscos residuais são elevados. Conforme dispõe no n.º 1 ao artigo 35.º, a realização de uma AIPD é obrigatória quando uma operação de tratamento "for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares".

Como também já salientamos, é da responsabilidade do responsável pelo tratamento de dados avaliar os riscos para os direitos e as liberdades dos titulares dos dados e identificar as medidas previstas para reduzir esses riscos para um nível aceitável e demonstrar a conformidade com o RGPD (als. c) e d) do n.º 7 do artigo 35.º e n.º 1 do artigo 24.º).

O GT29 esclarece, a este respeito, que nos casos em que não seja possível dar uma resposta cabal aos riscos identificados pelo responsável pelo tratamento (por não encontrar medidas suficientes para a mitigação dos riscos residuais e estes

[301] GT29 - Orientações sobre os encarregados da proteção de dados (WP 243rev.01), 13 dez 2016, revistas, por último, a 5 abr. 2017, p. 20. [Em linha]. Disponível em https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf

[302] GT29 - Orientações sobre os encarregados da proteção de dados. Op. Cit. p. 21.

permanecem elevados) é que se deve consultar a autoridade de controlo (n.º 1 do artigo 36.º). A título de exemplos de um risco residual inaceitavelmente elevado, o GT29 considera os casos em que os titulares dos dados podem sofrer consequências significativas, ou mesmo irreversíveis, que podem não conseguir superar (p. ex. um acesso ilícito a dados que possam vir a constituir uma ameaça para a vida dos titulares dos dados, um despedimento, uma ameaça financeira) e/ou casos em que pareça óbvio que o risco se irá concretizar (p. ex. não ser possível reduzir o número de pessoas que podem aceder aos dados devido aos modos de partilha, utilização ou distribuição utilizados ou quando uma vulnerabilidade conhecida não é solucionada)[303].

Desta forma, este regime introduz equilíbrio face à eliminação da anterior obrigação geral de notificação dos tratamentos às autoridades de proteção de dados que se encontrava na D 95/46, pelo que a comunicação às autoridades se limita agora às operações de tratamento que impliquem elevado risco para os direitos e liberdades das pessoas singulares (n.º 1 do artigo 36.º).

Contudo, importa referir que, independentemente de a consulta à autoridade de controlo ser ou não obrigatória com base no nível de risco residual, as obrigações que impõem a manutenção de um registo da AIPD e a atualização da AIPD em devido tempo permanecem válidas.

Além disso, os Estados-Membros devem assegurar a consulta da autoridade de controlo na elaboração de medidas legislativas ou regulamentares relacionadas com o tratamento de dados (n.º 4 do artigo 36.º).

Finalmente, o responsável pelo tratamento deve consultar a autoridade de controlo sempre que o direito do Estado-Membro exija que os responsáveis pelo tratamento consultem a autoridade de controlo e/ou dela obtenham uma autorização prévia em relação ao tratamento por um responsável no exercício de uma missão de interesse público, incluindo o tratamento por motivos de proteção social e de saúde pública (n.º 5 do artigo 36.º).

2.10. Poderes da Autoridade de Controlo

No âmbito da consulta, a autoridade de controlo pode, se entender que o tratamento violaria o RGPD, nomeadamente por o responsável não ter identificado ou atenuado suficientemente os riscos, dar orientações, por escrito, no longo prazo de oito semanas a contar da receção do pedido de consulta, ao responsável pelo tratamento e ao subcontratante, podendo ainda recorrer a todos os poderes previstos no artigo 58.º (n.º 2 do artigo 36.º).

A não realização da AIPD quando obrigatória, nos termos do artigo 35.º, bem como da consulta prévia à autoridade de controlo, nos termos do artigo 36.º, constituem contraordenações suscetíveis de aplicação de coimas até €10.000.000 ou, em caso de empresa, até 2% do volume anual de negócios a nível mundial conforme disposto na al. a) do n.º 4 do artigo 83.º.

Visitadas as fases da elaboração da avaliação de impacto, podemos compreender melhor a dinâmica relativa à necessidade de realização de uma AIPD

[303] GT29 - Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados, Op. Cit. p. 22.

com base no fluxograma abaixo que pretende ilustrar, esquematicamente, os passos a seguir.

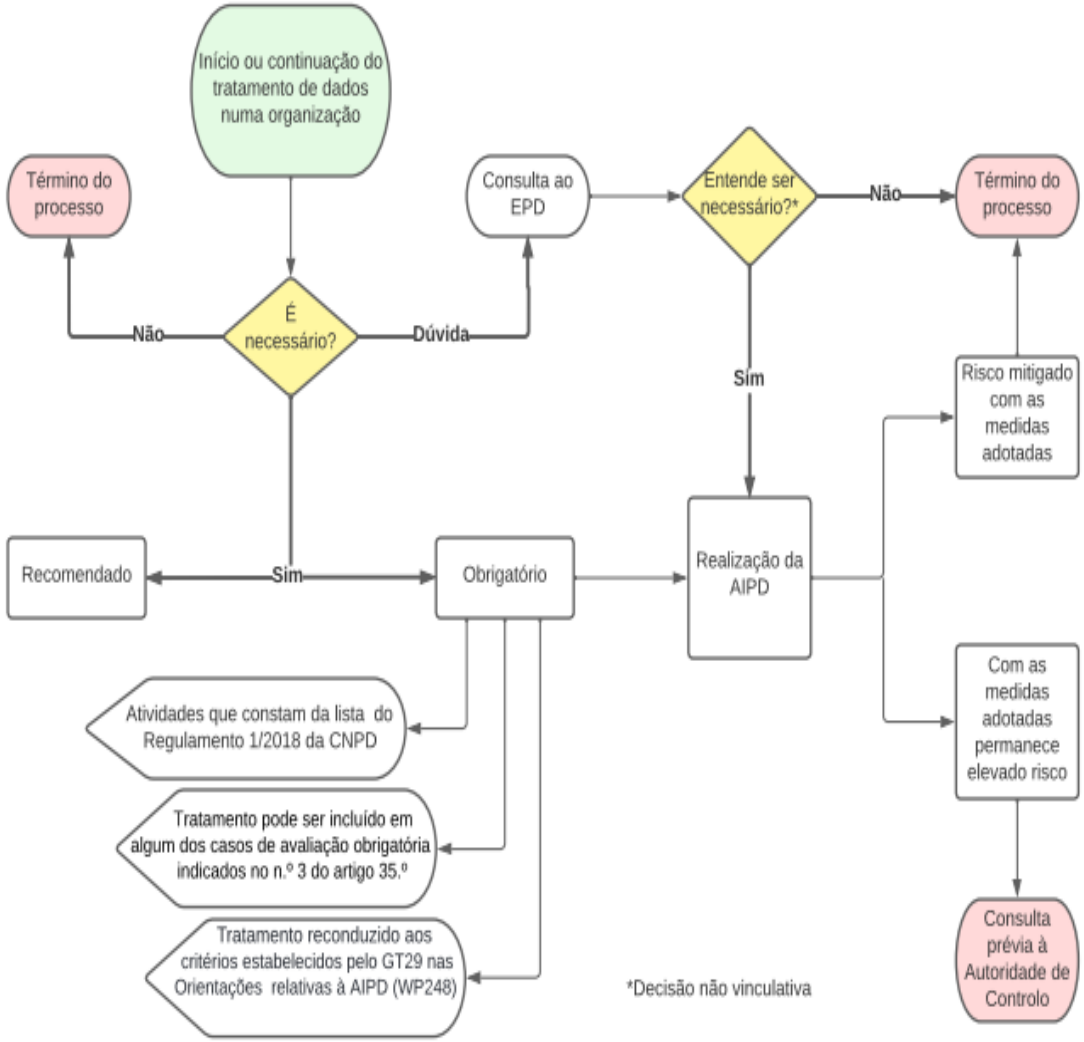


Fig. 2 – Fluxograma ilustrativo da dinâmica relativa à realização de AIPD
Elaborado pelo autor, abr. 2022

3. INFLUÊNCIA CRESCENTE DA AIPD NOS FUTUROS REGULAMENTOS

3.1. Proposta de Regulamento e-Privacy

Como acima já salientamos, uma AIPD é, no essencial, um processo que visa estabelecer e demonstrar a conformidade do tratamento de dados com o RGPD. Constitui um poderoso instrumento de *accountability* ao dispor do responsável pelo tratamento e uma sólida base de apoio na tomada de decisão em relação ao tratamento de dados pessoais.

Vimos igualmente que a AIPD, ao abrigo do RGPD, é um instrumento que visa a análise e a gestão dos riscos para os direitos dos titulares dos dados, e, como tal, é uma avaliação na perspetiva da proteção destes últimos.

No entanto, a esfera de influência da AIPD começa a extravasar o âmbito do RGPD, sendo este apenas a "ponta do iceberg" do contexto mais lato do ambiente digital na U.E..

Efetivamente, existe um conjunto de propostas de regulamentos que, não obstante dependerem da conclusão do processo legislativo europeu, já estão suficientemente maturadas e densificadas para se poder compreender o papel que a AIPD poderá assumir na futura regulação.

Um desses casos é a Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas) ou, mais vulgarmente designada, Proposta de Regulamento e-Privacy[304].

Logo no Considerando 5 da referida Proposta alerta-se que "(…) as disposições do presente regulamento precisam e completam as regras gerais relativas à proteção dos dados pessoais estabelecidas no Regulamento (UE) n.º 2016/679 no que respeita aos dados de comunicações eletrónicas que possam ser considerados dados pessoais. O presente regulamento, por conseguinte, não baixa o nível de proteção de que beneficiam as pessoas singulares ao abrigo do Regulamento (UE) 2016/679 (…)".

Portanto, o legislador europeu pretende manter o elevado grau de proteção dos dados pessoais conferido pelas regras gerais estabelecidas no RGPD e, desta forma, manter aplicáveis os mecanismos previstos para a proteção dos direitos dos titulares dos dados, incluindo, a previsão da necessidade de realização de AIPD.

Parece ser esse o caso dos tratamentos de metadados das comunicações eletrónicas pelos prestadores de serviços desse tipo de comunicações. Assim, no Considerando 17 da Proposta prevê-se que "(…) sempre que um tipo de tratamento de metadados de comunicações eletrónicas, nomeadamente que utilize novas tecnologias, e tendo em conta a natureza, o âmbito de aplicação, o contexto e as finalidades do tratamento, seja suscetível de conduzir a um elevado risco para os direitos e liberdades das pessoas singulares, deve realizar-se uma avaliação de impacto sobre a proteção dos dados e, se for caso disso, uma consulta da autoridade de controlo antes do tratamento, em conformidade com os artigos 35.º e 36.º do Regulamento (UE) 2016/679."

3.2. Proposta de Regulamento Inteligência Artificial

Na Proposta de Regulamento que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial)[305], à semelhança do RGPD, é evidente a prevalência da abordagem baseada no risco.

---

[304] Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas). [Em linha]. (10-01-2017). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52017PC0010

[305] Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera

A finalidade do futuro Regulamento é melhorar o funcionamento do mercado interno mediante o estabelecimento de um quadro jurídico uniforme para o desenvolvimento, a comercialização e a utilização da inteligência artificial (IA) em conformidade com os valores da União.

A Proposta de Regulamento segue uma abordagem baseada no risco e diferencia entre as utilizações de IA que criam: i) um risco inaceitável, ii) um risco elevado, iii) um risco baixo ou mínimo.

O título II da Proposta de Regulamento estabelece uma lista de práticas de IA proibidas. A referida lista inclui todos os sistemas de IA cuja utilização seja considerada inaceitável por violar os valores da União, por exemplo, por violar os direitos fundamentais.

O título III inclui regras específicas relativas aos sistemas de IA que criam um risco elevado para a saúde e a segurança ou para os direitos fundamentais de pessoas singulares. Em conformidade com uma abordagem baseada no risco, esses sistemas de IA de risco elevado são autorizados no mercado europeu, mas estão sujeitos ao cumprimento de determinados requisitos obrigatórios e a uma avaliação da conformidade *ex ante*. Existe igualmente uma lista de sistemas de IA de risco elevado constante do anexo III que inclui um número limitado de sistemas de IA cujos riscos já se materializaram ou são suscetíveis de se materializar num futuro próximo, podendo a Comissão alargar a referida lista em determinados domínios predefinidos, mediante a aplicação de um conjunto de critérios e de uma metodologia de avaliação de riscos.

O título IV abrange determinados sistemas de IA para ter em conta os riscos específicos que a manipulação dos mesmos representa. Aplicar-se-ão obrigações de transparência aos sistemas que: i) interagem com seres humanos, ii) são utilizados para detetar emoções ou determinar a associação com categorias (sociais) com base em dados biométricos, iii) geram ou manipulam conteúdos («falsificações profundas»).

O n.º 6 do artigo 29.º da Proposta de Regulamento vem estabelecer que "os utilizadores de sistemas de IA de risco elevado devem usar as informações recebidas nos termos do artigo 13.º para cumprirem a sua obrigação de realizar uma avaliação de impacto sobre a proteção de dados nos termos do artigo 35.º do Regulamento (UE) 2016/679 ou do artigo 27.º da Diretiva (UE) 2016/680, conforme aplicável".

Perante o exposto, é percetível a influência que o RGPD e, em concreto, a AIPD acaba por ter na definição da estrutura e do modelo de avaliação de risco contido na Proposta de Regulamento em análise, o que se compreende pela prioridade que, em ambos os casos, assume a proteção dos direitos e das liberdades dos titulares dos dados pessoais.

CONCLUSÃO

Com a entrada em vigor do RPGD verificou-se um reforço dos princípios já plasmados na D 95/46, assim como a consagração de novos princípios orientadores da conduta dos sujeitos obrigados ao tratamento de dados. Os princípios da "licitude, lealdade e transparência", da "limitação das finalidades", da "minimização de dados", da "exatidão", da "limitação da conservação", da "integridade e da confidencialidade"

determinados atos legislativos da União. [Em linha]. (21-04-2021). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

e da "responsabilidade" são de cumprimento obrigatório e constituem-se como verdadeiros pilares do quadro normativo relativo à proteção de dados pessoais.

O princípio da responsabilidade opera a dois níveis: (i) o responsável pelo tratamento deve atuar sempre no estrito cumprimento dos princípios elencados no n.º 1 do artigo 5.º; e (ii) o responsável pelo tratamento deve conseguir demonstrar, *maxime* às autoridades de controlo e aos tribunais, o cumprimento desses princípios. A AIPD aparece como um instrumento que o responsável pelo tratamento tem ao seu dispor para a materialização do princípio da responsabilidade, nomeadamente, do segundo nível, isto é, a demonstração de cumprimento ou daquilo que na versão inglesa do RGPD se denomina de *accountability*.

A AIPD ajuda os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas adequadas para assegurar a conformidade com o Regulamento, sendo, como bem sintetiza o GT29, um processo que visa estabelecer e demonstrar conformidade.

O responsável pelo tratamento é aquele que tem a obrigação de garantir a realização da avaliação de impacto (n.º 2 do artigo 35.º). Ainda que possa confiar esta tarefa a outras pessoas, dentro ou fora da organização, continua a ser o responsável último pela sua realização.

A AIPD deve ser efetuada antes de iniciar o tratamento e deve ser encarada como um instrumento de apoio à tomada de decisão do responsável em relação ao tratamento. No que respeita ao objeto pode abranger uma única operação de tratamento ou um conjunto de operações de tratamento semelhantes.

O RGPD não exige a realização de uma AIPD para todas as operações de tratamento que possam implicar riscos para os direitos e as liberdades das pessoas singulares, sendo apenas obrigatória quando o tratamento for "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (artigo 35.º, n.º 1, ilustrado pelo artigo 35.º, n.º 3, e complementado pelo artigo 35.º, n.º 4). Neste sentido, o RGPD adotou a abordagem baseada no risco, estabelecendo a obrigação de gerir o risco que um tratamento implica para os direitos e liberdades das pessoas singulares. Importa ter em conta que o foco da gestão do risco no RGPD é a proteção da pessoa, na sua dimensão individual e social, enquanto titular dos dados pessoais ou afetada pelo seu tratamento. Pelo que, a gestão de riscos para os direitos e liberdades não visa proteger os interesses do responsável ou responsáveis pelo tratamento em relação com este, por exemplo, quanto à continuidade do tratamento, sua eficácia ou sua eficiência, ou conformidade regulatória ou em relação às possíveis atividades comerciais do próprio responsável.

O RGPD permite que o responsável pelo tratamento determine como irá realizar a AIPD, tendo em conta a sua organização, de forma que possa ser adaptada às operações de tratamento e processos de negócio, todavia, estabelece o conteúdo mínimo que a AIPD deve incluir (n.º 7 do artigo 35.º). Contudo, seja qual for a sua forma, uma AIPD deve avaliar genuinamente os riscos, permitindo assim que os responsáveis pelo tratamento tomem medidas para dar resposta a esses riscos. Os responsáveis pelo tratamento não devem considerar a AIPD como um mero exercício formal e instantâneo

apenas para tentar demostrar conformidade junto da autoridade de controlo, mas como um instrumento ou um processo contínuo de genuína avaliação do risco.

Independentemente da metodologia utilizada, o GT29 estabeleceu, de acordo com as fases que a AIPD deve incluir, alguns critérios comuns que o modelo ou método escolhido pelo responsável pelo tratamento deve atender, a saber: a descrição sistemática das operações de tratamento, a avaliação da necessidade e da proporcionalidade do tratamento, a identificação das medidas previstas para demonstrar a conformidade, a avaliação dos riscos do tratamento para os direitos e liberdades dos titulares dos dados, as medidas para enfrentar os riscos, a documentação do processo, o controlo ou revisão e a audição dos interessados.

Ao efetuar uma AIPD, o responsável pelo tratamento deve solicitar o parecer do EPD. Pelo que, o referido parecer é obrigatório, a pedido do responsável pelo tratamento, se o EPD tiver sido designado. A autoridade de controlo deve ser consultada quando os riscos residuais são elevados (n.º 1 ao artigo 35.º), sendo certo que a não realização da AIPD quando obrigatória, nos termos do artigo 35.º, bem como da consulta prévia à autoridade de controlo, nos termos do artigo 36.º, constituem contraordenações suscetíveis de aplicação de coimas até €10.000.000 ou, em caso de empresa, até 2% do volume anual de negócios a nível mundial conforme disposto na al. a) do n.º 4 do artigo 83.º.

Por último, conclui-se que a esfera de influência da AIPD começa a extravasar o âmbito do RGPD, sendo este apenas a "ponta do iceberg" do contexto mais lato do ambiente digital na U.E. Efetivamente, existe um conjunto de propostas de regulamentos que, não obstante ainda dependerem da conclusão do processo legislativo europeu, já estão suficientemente maturadas e densificadas para se poder compreender o papel que a AIPD poderá assumir na futura regulação. Entre esses casos, assumem especial relevância a Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas) ou, mais vulgarmente designada, Proposta de Regulamento e-Privacy, bem como a Proposta de Regulamento que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial). Nas duas Propostas é percetível a influência que o RGPD e, em concreto, a AIPD acabam por ter na respetiva conceção e aplicação, o que bem se compreende pela prioridade que, em ambos os casos, assume a proteção dos direitos e das liberdades dos titulares dos dados pessoais.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Lurdes Dias – **Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador.** Coimbra: Edições Almedina, novembro de 2020. ISBN: 978-972-40-8581-4, p. 37.

ALVES, Tiago Rodrigues – Pirata vendeu dados de milhões de cartões bancários na Internet. **Jornal de Notícias**. Porto. (13 abr. 2022), p. 10.

ANDRADE, Rodrigo Rocha – **Da Responsabilidade do Encarregado da Proteção de Dados. Fórum da Proteção de Dados**. [Em linha]. N.º 7 (2020), p. 25. [Consult. 28 mar. 2022]. Disponível em https://www.cnpd.pt/media/5kajlbve/forum7_web.pdf.

Article 29 Data Protection Working Party - WP 203 - **Opinion 03/2013 on purpose limitation**. [Em Linha]. (Adotado a 2 de abril de 2013). Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Article 29 Data Protection Working Party - WP 218 - **Statement on the role of a risk-based approach in data protection legal frameworks**. [Em linha]. (Adotada a 30 de maio de 2014). [Consult. 28 de mar. 2022]. Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

Comité Europeu para a Proteção de Dados – **Parecer n.º 18/2018 sobre o projeto de lista da autoridade de controlo competente de Portugal respeitante às operações de tratamento de dados pessoais sujeitas a avaliação de impacto sobre a proteção de dados (artigo 35.º, n.º 4, do RGPD)**. [Em Linha]. (Adotado em 25 de setembro de 2018). Disponível em https://edpb.europa.eu/sites/default/files/files/file1/edps-2018-00017-00-14_pt.pdf.

Comité Europeu para a Proteção de Dados - **Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679** (versão 1.1), adotadas em 4 de maio de 2020. [Em Linha]. Disponível em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf.

CNPD – **Deliberação/2021/1569** aprovada na reunião de 21 de dezembro de 2021. [Em linha]. Lisboa. [Consult. 22 mar. 2022]. Disponível em https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-aplica-sancao-ao-municipio-de-lisboa/.

CORDEIRO, A. Barreto Menezes – **Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2019**. Coimbra: Edições Almedina, março de 2020. Reimpressão. ISBN 978-972-40-8304-9.

CORDEIRO, A. Barreto Menezes – **Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019**. Coimbra: Edições Almedina, março de 2021. ISBN 978-972-40-9261-4.

CORREIA, Gonçalo e CASANOVA, Rui - Laboratórios Germano de Sousa alvo de ataque informático. CUF alerta para "constrangimentos no acesso ao serviço de análises clínicas". **Observador**. (10 fev. 2022). [Consult. 20 mar. 2022]. Disponível em https://observador.pt/2022/02/10/laboratorios-germano-de-sousa-alvo-de-ataque-informatico/.

FRANCISCO, Daniel e FRANCISCO, Sandra – **Regulamento Geral de Proteção de Dados: 7 passos para uma metodologia de implementação do RGPD na Administração Pública**. Lisboa: Edições Sílabo, 2019. 1ª Edição. ISBN 978-989-561-014-3.

Grupo de Trabalho de Proteção de Dados do Artigo 29.º, WP 173 – **Parecer 3/2010 sobre o princípio da responsabilidade**, 13 de Jul. de 2010. [Em Linha]. Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/ wp173_pt.pdf.

Grupo de Trabalho de Proteção de Dados do Artigo 29.º, WP 187 – **Parecer 15/2011 sobre a definição de consentimento** (WP 187), 13 jul. 2011. [Em Linha]. Disponível em https://www.gpdp.gov.mo/uploadfile/others/wp187_pt.pdf.

Grupo de Trabalho de Proteção de Dados do Artigo 29.º, WP 243 - **Orientações sobre os encarregados da proteção de dados** (WP 243rev.01), 13 dez 2016, revistas, por último, a 5 abr. 2017. [Em linha]. Disponível em https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf.

Grupo de Trabalho de Proteção de Dados do Artigo 29.º, WP248 - **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679**. (WP 248rev.01), 4 abr. 2017, revistas, por último, a 11 out. 2017. [Em Linha]. Disponível em https://www.cnpd.pt/media/f0ide5i0/aipd_wp248rev-01_pt.pdf .

Grupo de Trabalho de Proteção de Dados do Artigo 29.º, WP 259 – **Orientações relativas ao consentimento na aceção do Regulamento (EU) 2016/679** (WP 259rev.01), 28 nov. 2017, revistas, por último, a 10 abr. 2018. [Em Linha]. Disponível em https://www.uc.pt/protecao-de-dados/suporte/20180410_orientacoes_relativas_ao_consentimento_wp259_rev01.

Grupo de Trabalho de Proteção de Dados do Artigo 29.º, WP 260 - **Orientações relativas à transparência na aceção do Regulamento 2016/679** (WP 260rev.1), 29 nov. 2017, revistas, por último, a 11 abr. 2018. [Em Linha]. Disponível em https://www.uc.pt/protecao-de-dados/suporte/20180411_orientacoes_relativas_a_transparencia_wp260_rev01.

LANÇA, Filomena - Russiagate: Lisboa cometeu 225 infrações com coimas máximas até 20 milhões. **Jornal de Negócios**. (01 jul. 2021). [Consult. 22 mar. 2022]. Disponível em https://www.jornaldenegocios.pt/economia/detalhe/russiagate-lisboa-cometeu-225-infracoes-com-coimas-maximas-ate-20-milhoes.

LOPES, Teresa Vale – **Responsabilidade e Governação das Empresas no Âmbito do Novo Regulamento de Proteção de Dados**. Anuário da Proteção de Dados 2018. Lisboa, 2018. [Em linha]. p. 54. [Consult. 7 mar. 2022]. Disponível em http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf.

MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão – **Regulamento Geral de Proteção de Dados – Manual Prático.** 3ª Edição Revista e Ampliada. Porto: Vida Económica, janeiro de 2020. ISBN: 978-989-768-680-1.

NOGUEIRA, Mariana Almeida – Quando o vírus é digital: os maiores ciberataques da História. **Visão**. Lisboa. (6 jan. 2022), p. 41-45.

Organização de Cooperação e Desenvolvimento Económico - **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. [Em linha]. Disponível https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1648644605&id=id&accname=guest&checksum=DC0AE8ED7821150A25BCD3DF6A4EF883.

RATO, Maria Moreira – Dark Web. E se o seu cartão de crédito estivesse à venda? **Jornal i**. [sl]. (24 fev. 2022). p. 16-18.

RODRIGUES, José Noronha e TEVES, Daniela Medeiros – **A Proteção de Dados Pessoais e a Administração Pública. O Novo Paradigma Jurídico**. Lisboa. AAFDL Editora, 2020. ISBN 978-972-629-543-3.

RODRIGUES, José Varela – Impresa avalia "impacto potencial" do ciberataque e toma "medidas necessárias. **Dinheiro Vivo**. Diário de Notícias. (5 jan. 2022). [Consult. 20 mar. 2022]. Disponível em https://www.dn.pt/media/impresa-avalia-impacto-potencial-do-ciberataque-e-toma-medidas-necessarias-14465275.html.

SÉNECA, Hugo – Sites do SNS enviam dados para a Google. **Expresso**. Lisboa. (25 de jun. 2021), p. 8.

SILVA, Hugo Tavares – A quem pertencem os dados? Primeiro Caderno. **Expresso**. Lisboa. (06 nov. 2021), p. 36.

VELHO, Marta – Vodafone Portugal foi alvo de ataque informático. Jornal de Negócios. (8 fev. 2022). [Consult. 20 mar. 2022]. Disponível em https://www.jornaldenegocios.pt/empresas/detalhe/vodafone-portugal-foi-alvo-de-ataque-informatico.

VÉLIZ, Carissa – **Privacidade é Poder, Por que razão e como devemos recuperar o controlo dos nossos dados**. Tradução de Pedro Vidal. Temas e Debates – Círculo de Leitores, 2022. ISBN 978-989-644-688-8,

ZUBOFF, Shoshana – **A Era do Capitalismo da Vigilância, A disputa por um futuro humano na nova fronteira do poder**. Tradução de Luís Filipe Silva e Miguel Serras Pereira. Relógio D'Água Editores, 2020. ISBN 978-989-783-090-7.

ATOS NORMATIVOS (E PROPOSTAS)

REGULAMENTO (UE) 2016/679. **Jornal Oficial da União Europeia**. [Em linha]. (04-05-2016), p. L119/1-119/88. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT.

Lei n.º 58/2019. **Diário da República, Série I**. N.º 151/2019 (08-05-2019), p. 3-40. [Em linha]. Disponível em https://dre.pt/web/guest/pesquisa/-/search/123815982/details/normal?_search_WAR_drefrontofficeportlet_print_preview=print-preview.

Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas). [Em linha]. (10-01-2017). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52017PC0010.

Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União. [Em linha]. (21-04-2021). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

JURISPRUDÊNCIA

ALMEIDA, Luís Nunes de Relat. - **Acórdão do Tribunal Constitucional n.º 634/93** – Processo nº 94/92. [Em linha]. [Consult. 26 abr 2022]. Disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19930634.html.

III_Legislação e Jurisprudência Comentadas

Comentário ao Acórdão do Tribunal da Relação do Porto relativo ao Processo 8233/21.0T8VNG.P1, de 8 de junho de 2022

Lurdes Dias Alves[306]

I – O caso em análise

Em 8 de junho de 2022, o Tribunal da Relação do Porto (TRP) decidiu, relativamente ao Recurso de apelação do Processo n.º 8233/21.0T8VNG.P1[307] (Procedimento cautelar de suspensão do despedimento), que, a empresa demandada agiu com licitude ao instaurar um procedimento disciplinar, o qual culminou com o despedimento com justa causa.

Fundamentando que, o arguido desobedeceu ilegitimamente às ordens emanadas pela entidade patronal, demonstrou desinteresse repetido pelo cumprimento, com a diligência devida, de obrigações inerentes ao exercício do cargo ou posto de trabalho a que está afeto e lesou gravemente interesses patrimoniais sérios da entidade patronal; assumindo comportamentos que, pela sua gravidade, consequências e grau de culpa do arguido, tornaram irremediável e praticamente impossível a subsistência da relação de trabalho, constituindo justa causa de despedimento.

O TRP decidiu improceder o recurso e manter a decisão recorrida.

---

[306] Licenciada em Direito e pela Universidade Autónoma de Lisboa. Pós-graduada em Direito Comercial e Direito Societário pela Universidade Católica Portuguesa – Escola de Lisboa. Mestre em Direito (especialidade de Ciências Jurídicas) pela Universidade Autónoma de Lisboa. Doutoranda em Direito (especialidade de Ciências Jurídicas) na Universidade Autónoma de Lisboa, onde investiga o tema: "*A proteção de dados pessoais e o sigilo bancário – A derrogação da privacidade*". Investigadora integrada no RATIO LEGIS - Centro de Investigação e Desenvolvimento em Ciências Jurídicas da Universidade Autónoma de Lisboa. Coordenadora de Pós-Graduações em: Proteção de Dados Pessoais, Privacidade e Cibersegurança na EU; e Prevenção e Deteção de Fraude Empresarial, na Autónoma Academy (Escola de Pós-graduações da Universidade Autónoma de Lisboa). Professora universitária convidada na Universidade Autónoma de Lisboa. Autora de várias publicações e participante regular em iniciativas públicas de Direito do trabalho e Proteção de Dados. Consultora Jurídica.

[307] Acórdão do Tribunal da Relação de Coimbra de 8 de junho de 2022 (Proc.º 38233/21.0T8VNG.P1). Relator: Desembargador António Luís Carvalhão. [em linha]. Consultado em 29 de agosto de 2022. Disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/8d1e1c580ca5251a80258864004c1b66?OpenDocument

II - Factualidade

Um motorista de táxi de uma empresa de viaturas ligeiras destinadas ao transporte de passageiros, semanalmente, tal como todos os motoristas da empresa, deslocava-se às instalações da entidade patronal, onde entregava a uma outra trabalhadora (indicada pela gerência), os valores em dinheiro que tinha na sua posse, referente ao apuro dos serviços efetuados com o táxi que conduzia durante aquela semana e, bem assim as despesas de gasóleo, portagens ou outras.

Nessas deslocações, eram verificados os valores em dinheiro entregues, os valores em euros registados no taxímetro e, bem assim, o número de quilómetros registado no conta-quilómetros do veículo. Para de seguida, se confrontar os dados recolhidos da aplicação X... (percursos realizados) com os dados recolhidos da leitura do taxímetro (valores recebidos pelo motorista) e do conta-quilómetros.

Acontece que, em fevereiro de 2021, foram detetadas pela empresa incongruências entre os valores entregues pelo motorista e o apuramento efetuado na aplicação X… Constatou-se que o motorista fez vários percursos com o taxímetro no estado Livre e no estado de Pausa, outros até, com o taxímetro totalmente desligado e nalguns deles – devidamente identificados nos autos – o motorista durante o mesmo percurso foi mudando o taxímetro do estado Ocupado ou Recolha da Central para o estado Livre ou Pausa por diversas vezes.

Em todos esses percursos o arguido cobrou do cliente e, por vezes emitiu, até, a respetiva fatura. Sabendo, pela sua experiência profissional, que o taxímetro quando está no estado Livre ou Pausa não está a contar; ou seja, não regista qualquer valor em euros no taximetro. Tinha perfeito conhecimento que ao circular com o taxímetro no estado Livre ou Pausa ou, até, desligado, o valor do serviço inerente aos quilómetros assim percorridos não ficaria registado no taxímetro; e, como tal, no final da semana, tal valor não era contabilizado pela entidade patronal, entregando, somente, a quantia exata, *i.e.*, o valor que constava do taxímetro (mais concretamente, a diferença entre o valor registado e o que havia sido registado na semana anterior).

Pelo que, a entidade empregadora instaurou um procedimento disciplinar que culminou no despedimento por justa causa.

O motorista não conformado com o despedimentos por justa causa, decidiu instaurar um Procedimento cautelar de suspensão do despedimento, o qual foi pelo Tribunal *a quo* proferida sentença julgando o procedimento cautelar improcedente, indeferindo a suspensão do despedimento. Não se conformando interpôs o recurso cuja decisão se concretiza no presente acórdão.

III - Apreciação do Tribunal da Relação do Porto

I - O regime previsto na cláusula 50ª do CCT celebrado entre a ANTRAL e a FESTRU, que prevê a comunicação da intenção de proceder disciplinarmente e o prazo de 5 dias úteis para deduzir «nota de culpa» cede perante a imperatividade do regime legal da «cessação do contrato de trabalho», e como tal o prazo para o início do procedimento disciplinar é o previsto no art.º 329º, nº 2, do Código do Trabalho.

II - A instalação de sistema de geolocalização em táxi, sem visar o controlo do desempenho do motorista (trabalhador), e sem pôr em causa a esfera de privacidade e reserva do motorista (trabalhador), pode ser admitido como meio de prova no procedimento disciplinar.
III - É esse o caso de semanalmente ser feito o apuro de cada motorista de táxi, e conferidas as contas (se os valores recebidos correspondem com os percursos percorridos, não avaliar o desempenho do motorista), conjugando os dados recolhidos da aplicação X... (percursos realizados) com os dados recolhidos da leitura do taxímetro (valores recebidos pelo motorista) e do conta-quilómetros.

IV - Comentário

Delimitamos o presente comentário à instalação de sistema de geolocalização em táxi e da conjugação dos dados recolhidos do taxímetro instalado no veículo, sistema de geolocalização e número de quilómetros percorridos por semana e aferidos na aplicação X.

Do Douto Acórdão resulta que, a instalação de sistema de geolocalização em táxi, sem visar o controlo do desempenho do motorista (trabalhador), e sem pôr em causa a esfera de privacidade e reserva do motorista (trabalhador), pode ser admitido como meio de prova no procedimento disciplinar.

Na verdade, o sistema, instalado no veículo, não se destinava, nem tinha aptidão para vigiar e controlar o desempenho profissional do trabalhador e muito menos a sua vida pessoal pese embora pudesse acompanhar os percursos dos veículos em serviço de táxi das empresas a ele aderentes[308]. Serve somente para «contabilizar» as distâncias percorridas e os valores registados nos taxímetros e seu estado de ocupado, livre, em pausa ou desligado.

O veículo não dispunha de qualquer sistema de captação de imagem e som e era do conhecimento dos motoristas dos veículos a ele ligados, como era o caso do Recorrente.

Nessas condições, tal sistema de georreferenciação não pode sequer ser considerado meio de vigilância à distância, tal como previsto e regulado nos artigos 20º e 21º do Código do Trabalho.

Veja-se o Acórdão do Supremo Tribunal de Justiça de 13 de novembro de 2013[309]: O dispositivo de GPS instalado, pelo empregador, em veículo automóvel utilizado pelo seu trabalhador no exercício das respetivas funções, não pode ser qualificado como meio de vigilância à distância no local de trabalho, porquanto apenas permite a localização do veículo em tempo real, não permitindo saber o que faz o respetivo condutor. Encontrando-se o GPS instalado numa viatura exclusivamente afeta às necessidades do serviço, não permitindo a captação ou registo de imagem ou som[310], o seu uso não ofende os direitos de personalidade do trabalhador, nomeadamente a reserva da intimidade da sua vida privada e familiar.

---

[308] Por intermédio da cooperativa que o adotara.

[309] **Acórdão do Supremo Tribunal de Justiça** de 13 de novembro de 2013 (Proc.º 73/12.3TTVNF.P1.S1). Relator: Conselheiro Mário Belo Morgado. [em linha]. Consultado em 14 de setembro de 2022. Disponível em: www.dsgi.pt

[310] Sublinhado nosso

Tal como temos vindo a «defender»[311], há várias tecnologias que permitem reconhecer, cada vez com maior precisão, a localização geográfica de um objeto e/ou uma pessoa, destacando-se a tecnologia GPS (*Global Positioning System*), utilizada com frequência em veículos automóveis; os dados de geolocalização são dados pessoais, e no contexto laboral exige-se que a utilização dessa tecnologia ocorra com especial cautela, sendo a preocupação principal a de que a utilização descomprometida e excessiva desses dispositivos viole direitos fundamentais dos trabalhadores, especialmente a reserva da vida privada.

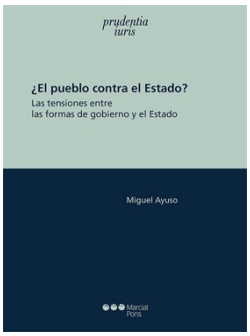
Com efeito, os dados de geolocalização, apesar de não estarem expressamente previstos, são dados sensíveis[312], na medida que podem «*fragilizar*» o direito à privacidade do trabalhador. Contudo, é admitida a instalação de sistemas de geolocalização em automóveis para gestão de serviços de frota em serviço externo na atividade de transporte de passageiros, desde que não usados para controlar o desempenho do trabalhador.

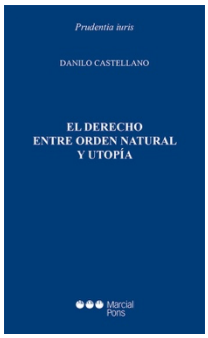
---

311 Cfr. ALVES, Lurdes Dias – **Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador**. Coimbra: Edições Almedina, junho de 2020. P. 34. E foi, precisamente, neste sentido, a decisão do presente acórdão nesta matéria, em que nos cita a nota (41).

312 Como já o era nos termos e para os efeitos do disposto no n.º 1 do art.º 7.º da Lei n.º 67/98, de 26 de Outubro, uma vez que o tratamento de dados pessoais resultantes de geolocalização tem de ser efetuado com precauções especiais, assim *"(…) no âmbito do tratamento notificado, pretende-se efetuar um tratamento de dados pessoais decorrentes de geolocalização. O dado «localização» subsume-se ao conceito de dado relativo à vida privada e, nessa medida, é qualificado como dado sensível (…)"*.

IV_Recensões





Notícia Bibliográfica

Pedro Rebelo Botelho Alfaro Velez[313]

Ayuso, Miguel, *¿El pueblo contra el Estado? Las tensiones entre las formas de gobierno y el Estado*, Marcial Pons, Madrid, 2022 (145 pp.).

Castellano, Danilo, *El Derecho entre orden natural y utopia*, Marcial Pons, Madrid, 2022 (197 pp.).

Em mais uma obra de reativação da tradição da filosofia política e jurídica de derivação clássica, o constitucionalista Miguel Ayuso (catedrático da Faculdade de Direito da Universidade Pontifícia Comillas de Madrid) procura analisar criticamente a atual *episteme* político-jurídica, problematizando as noções hegemónicas de comunidade política (ou melhor, de Estado – determinação moderna da comunidade política), de Povo, de Direito Público e em sede de formas de governo, mormente no que toca à definição e à articulação dos conceitos de Democracia e de Monarquia. A categorias expostas ou descodificadas como em estado de crise radical ou como eivadas de aporias, o autor contrapõe uma redescoberta, com todas as consequências de ordem jurídico-política, da «comunidade política natural»: «aquela em que a justiça é elemento ordenador intrínseco da comunidade humana».

Numa linha convergente de teorização e de problematização, Danilo Castellano, catedrático de Filosofia Política da Universidade de Udine, pôde, também recentemente, reexaminar as estruturas profundas da experiência e da prática jurídicas contemporâneas. Segundo o jusfilósofo, ao entendimento dominante sobre o direito e os direitos subjaz uma noção de «*liberdade negativa*»: uma liberdade que apenas teria como critério a própria liberdade, ou seja, a ausência de uma regra substantiva. Acompanhando o discurso dos direitos humanos e fundamentais de derivação liberal, tal compreensão matricial manifestar-se-ia hodiernamente em termos de acabada realização, nos chamados «novíssimos direitos». A uma utópica «autodeterminação como autonomia absoluta» opõe-se uma visão clássica da jurisprudência enquanto determinação do que é conforme à justiça, atendendo «à natureza das coisas».

313 **Pedro Rebelo Botelho Alfaro Velez**, Professor da Universidade Europeia, Professor convidado no Instituto Politécnico de Leiria. Membro do centro de investigação CEDIS (Nova Direito). Nascido a 26.11.1979. Licenciado em Direito pela Faculdade de Direito da Universidade Nova de Lisboa (2002). Doutor em Direito (fevereiro de 2014), na especialidade de Ciências Políticas, também pela FDUNL. Nos últimos anos, tem-se dedicado à investigação e ao ensino, lecionando disciplinas de direito público (direito constitucional e direito administrativo) e de índole históricojurídica (história das instituições portuguesas, história do Estado), na FDUNL, na Universidade Europeia, na Escola de Direito da Universidade Católica Portuguesa-Porto, bem como no Instituto Politécnico de Leiria. Áreas de interesse: tipos históricos de Estado, formas políticas, regimes políticos/formas de governo e sistemas de governo, constitucionalismo, relações entre o políticoconstitucional e o religioso.