ANUÁRIO
DA PROTEÇÃO DE DADOS
2020

COORDENAÇÃO
FRANCISCO PEREIRA COUTINHO
GRAÇA CANTO MONIZ

CEDIS
CEDIS CENTRO DE I&D
SOBRE DIREITO E SOCIEDADE

ANUÁRIO
DA PROTEÇÃO DE DADOS
2020

ANUÁRIO DA PROTEÇÃO DE DADOS

2020

COORDENAÇÃO
FRANCISCO PEREIRA COUTINHO
GRAÇA CANTO MONIZ

CEDIS
CEDIS CENTRO DE I&D
SOBRE DIREITO E SOCIEDADE

ANUÁRIO DA PROTEÇÃO DE DADOS 2020

COORDENAÇÃO

Francisco Pereira Coutinho
Graça Canto Moniz

SECRETÁRIA EXECUTIVO

João Marques de Azevedo

EDIÇÃO

Universidade Nova de Lisboa. Faculdade de Direito.
CEDIS, Centro de I & D sobre Direito e Sociedade
Campus de Campolide, 1099-032 Lisboa, Portugal

SUPORTE: ELETRÓNICO

Junho, 2020

ISSN 2184-5468

CATALOGAÇÃO NA PUBLICAÇÃO

PEREIRA COUTINHO, Francisco e CANTO MONIZ, Graça (coord.). Anuário da Proteção de Dados 2020. Lisboa: CEDIS, 2020

Nota Introdutória

O Anuário da Proteção de Dados é uma revista jurídica de livre acesso, disponível em linha no sítio https://protecaodedadosue.cedis.fd.unl.pt, que pretende divulgar estudos doutrinários sobre o direito da proteção de dados pessoais. A revista é editada desde 2018 pelo Observatório da Proteção de Dados Pessoais, um grupo de investigação criado em 2016 no CEDIS – Centro de I & D sobre Direito e Sociedade da *Nova School of Law*.

Os cinco artigos publicados na edição de 2020 do Anuário resultam de uma chamada lançada em setembro de 2019 no sítio da internet do Observatório da Proteção de Dados Pessoais. Os textos foram depois sujeitos a um processo de *blind peer review* e posteriormente revistos pelos coordenadores do Anuário. Aos autores foi permitido escreverem de acordo com a nova ou a antiga grafia.

O Anuário inicia-se com um texto da autoria do Francisco Pereira Coutinho sobre a independência da Comissão Nacional de Proteção de Dados Pessoais, seguindo-se um artigo do Augusto Torbay que trata o tema da anonimização enquanto mecanismo de proteção de dados pessoais. Os direitos do titular dos dados são o tema que se segue, em particular em relação a decisões algorítmicas, num texto da autoria da Beatriz Trindade. A Francisca Gomes, debruça-se sobre o mesmo tema, mas segundo uma perspetiva diferente, isto é, procurando explicar o conteúdo do direito fundamental à proteção de dados pessoais. Por último, a Patrícia Santos, escreve sobre o tema dos prazos de conservação de dados pessoais dos candidatos a emprego.

Esta obra não teria sido possível sem o patrocínio da SRS Advogados e da FUTURA, a quem agradecemos, nas pessoas do Luís Neto Galvão (SRS Advogados) e do Rodrigo Adão da Fonseca (FUTURA), o apoio que têm prestado desde a primeira hora a este projeto. Igualmente devidos

são agradecimentos aos revisores deste número, o André Inácio, o Danilo Doneda, o João Traça, a Helena Tapp Barroso, a Inês Oliveira, o Luís Neto Galvão, a Magda Cocco, o Martinho Lucas Pires, o Matheus Passos Silva, o Ricardo Rodrigues Oliveira e o Rui Lanceiro. Por fim, agradecemos ao João Marques de Azevedo o auxílio prestado na edição do Anuário, bem como a todos os autores que participam nesta edição.

Lisboa, 28 de maio de 2020

Francisco Pereira Coutinho
Graça Canto Moniz
Coordenadores do Observatório da Proteção de Dados

Índice Sumário

A Independência da Comissão Nacional de Proteção de Dados

Francisco Pereira Coutinho*

Resumo: A Comissão Nacional de Proteção de Dados agitou as habitualmente plácidas águas da ordem jurídica portuguesa quando anunciou a decisão de desaplicar, com fundamento na violação do direito da União Europeia, várias disposições da muito aguardada e recentemente aprovada lei de execução do Regulamento Geral de Proteção de Dados. Este exercício do chamado "mandato *Costanzo*" constitui um exemplo de escola de supervisão independente por uma "guardiã do direito à proteção de dados" num Estado-Membro. Pode também ter sido o "canto do cisne" da Comissão Nacional de Proteção de Dados se o Estado português não cumprir a sua obrigação de a prover com os recursos de que necessita para cumprir eficazmente as múltiplas atribuições que lhe são conferidas pelo Regulamento Geral de Proteção de Dados.

Palavras-chave: *Autoridade de controlo nacional; Portugal; Primado; Proteção de Dados; Regulamento Geral de Proteção de Dados; União Europeia.*

Abstract: The Portuguese Data Protection Authority has shaken the Portuguese legal order's usually placid waters by vowing to disapply, based on the breach of European Union law, several provisions of the long-awaited and recently enacted law that implements the General Data Protection Regulation. This exercise of the so-called "*Costanzo* mandate" is

* Professor da Faculdade de Direito da Universidade Nova de Lisboa. Membro do CEDIS – Centro de I & D sobre Direito e Sociedade, onde coordena o Observatório da Proteção de Dados e edita o Anuário da Proteção de Dados. Este texto desenvolve palestra apresentada na conferência "Desafios e Perspetivas das Autoridades de Proteção de Dados Pessoais e Privacidade", organizada na Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo, Brasil, a 8 de novembro de 2019. São devidos agradecimento ao Filipe Brito Bastos, à Graça Canto Moniz, ao Luís Neto Galvão e ao Rui Tavares Lanceiro pela leitura crítica deste texto, que muito o valorizou. Eventuais incorreções que nele se encontrem são da minha responsabilidade exclusiva.

a textbook example of independent supervision by a "guardian of data protection rights" in a Member State. It may also be the "swan song" of the Portuguese Data Protection Authority if the Portuguese State does not fulfil its obligation to provide the authority with the adequate resources needed to effectively fulfil its multiple tasks under the General Data Protection Regulation.

Passwords: *Data Protection; European Union; General Data Protection Regulation; Portugal; Supervisory authority; Supremacy.*

1. Crónica de uma decisão de desaplicação anunciada

I. A 16 de maio de 2018, nas vésperas do início da aplicação do Regulamento Geral de Proteção de Dados (RGPD)[1], a presidente da Comissão Nacional de Proteção de Dados (CNPD) declarou, numa audição parlamentar, que:

> "(...) Em junho (de 2018) já não há dinheiro para pagar os vencimentos dos trabalhadores da Comissão (Nacional de Proteção de Dados) (...). Nós, Estado português, que tivemos a primeira Constituição a consagrar o direito fundamental à proteção de dados, vamos passar pela vergonha de sermos aquele que não reforçou os meios da autoridade de proteção de dados, e que está praticamente obrigada a fechar portas quando o regulamento começar a ser aplicado"[2].

A notícia do encerramento iminente da entidade administrativa independente reconhecida como "a autoridade de controlo nacional" para

---

[1] O Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, é o ato legislativo da União Europeia que estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (art. 1.º, n.º 1, RGPD). É diretamente aplicável desde o dia 25 de maio de 2018, dois anos depois do início da sua vigência, que ocorreu a 24 de maio de 2016 (art. 99.º RGPD). O RGPD revogou a Diretiva 95/46/CE, de 24 de outubro de 1995.

[2] Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, "Audição de Filipa Calvão, Presidente da Comissão Nacional de Proteção de Dados, sobre a questão da cedência ilegítima de dados pessoais pela rede social Facebook, assim como sobre as diligências tomadas pela CNPD para garantir a proteção dos dados pessoais dos utilizadores portugueses desta e de outras redes sociais", 16 de maio de 2019, 24:39 a 24:56.

efeitos da fiscalização da aplicação do RGPD em Portugal[3], revelar-se-ia manifestamente exagerada, como o demonstra a aplicação de coimas de €400.000 a um hospital público, a 9 de outubro de 2018, e de €107.000 a uma empresa privada, a 6 de maio de 2019[4].

A prova de vida definitiva da CNPD surgiria a 3 de setembro de 2019 ao declarar que, de forma a assegurar o primado do direito da União e a efetividade do RGPD, não iria aplicar várias normas da lei de execução do RGPD, cuja vigência se tinha iniciado semanas antes, a 9 de agosto de 2019[5].

II. A adoção de uma lei de execução resulta de o RGPD obrigar os Estados-Membros a intervir legislativamente para implementar o regulamento[6]; acresce a circunstância de estarmos perante um ato legislativo da União que tem "o corpo de um regulamento, mas a alma de uma diretiva"[7], na medida em que reconhece aos Estados-Membros alguma margem de conformação normativa em vários domínios[8].

---

[3] Art. 3.º da Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica portuguesa, do Regulamento (UE) 2016/679 do Parlamento 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 ("lei de execução").

[4] Cfr., respetivamente, a Deliberação n.º 984/2018, de 9 de outubro, e a Deliberação n.º 297/2019, de 6 de maio. No relatório de atividades relativo aos anos de 2017 e 2018, a CNPD relata que, no período de aplicação do RGPD relativo ao ano de 2018, aplicou 22 coimas no valor total de €408 990,40, a maior parte das quais dizia respeito a factos praticados antes de 25 de maio de 2018, pelo que lhes foi aplicado o regime contraordenacional previsto na Lei Geral de Proteção de Dados (Lei n.º 67/98, de 26 de outubro), que previa molduras sancionatórias mais favoráveis aos arguidos (Comissão Nacional de Proteção de Dados, *Relatório de Atividades 2017/2018*, de 23 de abril de 2019, p. 28).

[5] Deliberação n.º 494/2019, de 3 de setembro, pp. 2-11.

[6] Por exemplo, escolhendo um organismo de acreditação com um nível adequado em matéria de proteção de dados (art. 43.º, n.º 1, RGPD).

[7] GARCÍA MEXÍA, Pablo, "La singular naturaleza jurídica del reglamento general de protección de datos de la EU. Sus effectos en el acervo nacional sobre protección de datos", in PIÑAR MAÑAS, José Luis (dir.), *Reglamento General de Protección de Datos – Hacia un nuevo modelo europeo de privacidad*, Reus, 2016, p. 34.

[8] *V. g.* o art. 8.º, n.º 1, RGPD, que permite que os Estados-Membros definam a idade com que as crianças podem ter acesso, sem carecer de consentimento dos seus representantes legais, à oferta direta de serviços da sociedade da informação, a qual pode variar entre 13 e 16 anos.

Portugal foi o antepenúltimo Estado-Membro da União Europeia a adotar legislação de implementação do RGPD[9]. O processo legislativo iniciou-se apenas em agosto de 2017 – quinze meses depois da entrada em vigor do RGPD e numa altura em que a Alemanha já tinha aprovado legislação federal de implementação do regulamento[10] – com a constituição de um grupo de trabalho a quem foi atribuída a tarefa de preparar a legislação requerida pelo RGPD[11]. Seguiu-se um processo de consulta pública que culminou com a apresentação de uma anteproposta de lei no final de 2017[12]. O Conselho de Ministros aprovou uma proposta de lei a 22 de março de 2018[13], tendo na altura a Ministra da Presidência e da Modernização Administrativa expressado o desejo de que "(seria) bom para todos que o RGPD e a proposta de lei pudessem estar disponíveis em simultâneo"[14]. A 3 de maio de 2018, a proposta foi objeto de críticas de natureza procedimental[15]

---

[9] De acordo com a Comissão Europeia, "GDPR Implementation. Update State of Play in the Member States (11/04/2019)", em abril de 2019 apenas a Eslovénia e a Grécia não tinham aprovado legislação de execução do RGPD. A lei grega (4624/2019) foi entretanto aprovada e publicada a 29 de agosto de 2019 (BROUMAS, Antonios, "GDPR Incorporated into Greek Law", *iapp*, 4 de outubro de 2019).

[10] *Bundesdatenschutzgesetz*, de 30 de junho de 2017.

[11] Despacho 7456/2017, de 24 de Agosto, da Presidência do Conselho de Ministros. A ausência de um representante da CNPD no grupo de trabalho foi criticada por MENEZES CORDEIRO, A. B., "Portugal: A Brief Overview of the GDPR Implementation", *European Data Protection Law Review*, 4, 2019, p. 536.

[12] O edital do processo de consulta pública pode ser consultado aqui.

[13] Ponto 1 do Comunicado do Conselho de Ministros de 22 de março de 2018.

[14] Conferência de Imprensa do Conselho de Ministros, de 22 de março de 2018, 11:38 a 11:40.

[15] Cfr. as intervenções da deputada Vânia Dias da Silva (CDS/PP), *Diário da Assembleia da República*, de 4 de maio de 2018, I Série, 80, p. 10 ["(...) é absolutamente inaceitável (...) que o Governo pressione o Parlamento para legislar à pressa numa matéria que já conhece há mais de dois anos e na qual há mais de dois anos poderia ter trabalhado. Não é aceitável, não é compreensível e nem sequer se entende o porquê (...) porque já todos conhecíamos esta matéria, todos sabíamos que o Regulamento entrava em vigor no dia 25 de maio (de 2018). O Regulamento previa uma moratória de dois anos para que todos se adaptassem. E o que aconteceu? O Governo ficou quieto, parado e à espera, não fez nada e, portanto, agora estamos todos a braços com problemas de implementação, que, obviamente, este Governo não quis acautelar não se entende bem porquê"], do deputado Carlos Abreu Amorim (PSD) *Diário da Assembleia da República*, de 4 de maio de 2018, I Série, 80, p. 11 ["O Regulamento

e substantiva[16] no plenário da Assembleia da República que, consequentemente, deliberou, por unanimidade, o seu regresso sem votação à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias[17]. Um texto de substituição da proposta de lei elaborado por esta Comissão foi (finalmente) aprovado pelo plenário da Assembleia da República a 14 de junho de 2019[18].

A CNPD participou nos trabalhos preparatórios da lei de execução através da apresentação de um extenso parecer sobre a proposta de lei e através da audição parlamentar da sua presidente, tendo-se pronunciado no sentido de que um número muito significativo de disposições da proposta de lei de implementação do RGPD violavam o direito da União Europeia[19].

III. O anúncio da recusa de aplicação de várias disposições previstas na lei de execução por uma entidade administrativa independente não foi bem recebido no parlamento. O presidente em exercício da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República (e também professor de direito constitucional), Pedro Bacelar de Vasconcelos, considerou estarmos perante uma decisão "inadmissível" porque "tomada de forma autónoma, sem sequer dar

---

Geral de Proteção de Dados é de 2016, mas a proposta que hoje debatemos só foi aprovada em Conselho de Ministros no final de março (de 2018) e só tivemos conhecimento dela em abril (de 2018). Foi tarde, muito tarde, para uma matéria com esta dimensão e impacto"] e do deputado António Filipe, *Diário da Assembleia da República*, de 4 de maio de 2018, I Série, 80, p. 13 ["A proposta de lei que hoje discutimos, destinada a assegurar a aplicação em Portugal do Regulamento Geral da União Europeia relativo à proteção de dados pessoais e à livre circulação desses dados, chegou tarde e a más horas a esta Assembleia (...). Perante uma matéria tão complexa, extensa e inegavelmente importante, dado que é matéria de direitos fundamentais, não é exigível que esta Assembleia discuta e aprove em 15 dias o que o Governo demorou dois anos para discutir e aprovar"].

[16] Cfr. *Diário da Assembleia da República*, de 4 de maio de 2018, I Série, 80, pp. 7-15.

[17] *Diário da Assembleia da República*, de 5 de maio de 2018, I Série, 81, p. 45.

[18] Com os votos favoráveis do PSD, do PS e do deputado não inscrito Paulo Trigo Pereira e a abstenção do BE, CDS-PP, PCP, PEV, PAN (*Diário da Assembleia da República*, de 15 de junho de 2019, I Série, 96, pp. 37 e 38).

[19] Parecer n.º 20/2018, de 2 de maio, e Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, "Audição da Comissão Nacional de Proteção de Dados", 27 de novembro de 2019, 00:58:56 a 01:01:10.

uma explicação prévia da desobediência perante o órgão de soberania a que (a CNPD) deve legitimidade", acrescentando que "(u)m órgão de autoridade do Estado que se coloca nesta posição ou se demite ou obtém (sic) esclarecimentos que justifiquem a sua continuidade. É algo que cabe ao parlamento decidir"[20].

Estas declarações comprometem o papel da CNPD enquanto "guardiã" do direito à proteção de dados na ordem jurídica portuguesa[21], resultante do mandato constitucional, previsto no art. 16.º, n.º 2, do Tratado sobre o Funcionamento da União Europeia (TFUE) e no art. 8.º, n.º 2, da Carta dos Direitos Fundamentais da União Europeia, de fiscalizar a observância das normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais. Revelam sobretudo desconhecimento da natureza das autoridades de controlo e, em particular, do estatuto de "total independência" de que estas estão investidas (art. 52.º, n.º 1, RGPD) (v. secção 2 deste artigo). Apresentam-se ainda particularmente graves porque têm origem num importante membro do órgão de soberania que manifestamente não tem provido a CNPD dos recursos necessários à prossecução eficaz das suas atribuições (art. 52.º, n.º 4, RGPD) (v. secção 3 deste artigo).

2. A independência das autoridades de controlo

2.1. A natureza das autoridades de controlo

A União Europeia organizou-se, desde a sua origem, de acordo com o princípio da subsidiariedade, que requer que as decisões sejam tomadas "ao nível mais próximo possível dos cidadãos" [art. 1.º do Tratado da União Europeia (TUE)].

O RGPD concretiza o princípio da subsidiariedade ao determinar que os Estados-Membros devem criar autoridades nacionais de fiscalização

---

[20] SÉNECA, Hugo, "Parlamento admite que CNPD tem legitimidade para não aplicar lei da proteção de dados. No PS, fala-se em demissão", *Exame Informática*, de 26 de setembro de 2019.

[21] Tribunal de Justiça (da União Europeia), acórdão de 9 de março de 2010, *Comissão c. Alemanha*, C-518/07, EU:C:2010:125, para. 23.

da proteção de dados com a missão "de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento (de dados pessoais) e facilitar a livre circulação desses dados na União" (art. 51.º, n.º 1). A rejeição de uma solução federal, através da instituição de uma autoridade europeia de controlo da aplicação do direito da União nestes domínios nos Estados-Membros[22], terá resultado, para além de razões históricas[23], do reconhecimento de que as autoridades de controlo nacionais estão melhor posicionadas para, por um lado, interpretar as especificidades e restrições a regras do RGPD previstas no direito nacional e, por outro, para levar a cabo o fundamental exercício casuístico de ponderação do direito à proteção de dados com outros direitos fundamentais, como a liberdade de expressão e o acesso à informação[24], e com objetivos de interesse geral, como a transparência e a segurança interna e externa, no quadro de um ambiente tecnológico em permanente evolução.

---

[22] Os poderes de supervisão independente da Autoridade Europeia para a Proteção de Dados estão circunscritos ao controlo da aplicação do direito da União relativo à proteção de dados pessoais por instituições ou órgãos da União [art. 52.º, n.ºs 2 e 3, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) 45/2001 e a Decisão 1247/2002/CE].

[23] A *Commission Nationale Informatique et Libertés* (CNIL), a primeira autoridade administrativa independente de supervisão do direito à proteção de dados pessoais, foi criada em França em 1978 (GONZÁLEZ FUSTER, Gloria, *The Emergence of Personal Data Protection as a Fundamental Right of the EU Law*, Springer, 2014, p. 65), muito antes de o art. 28.º, n.º 1, da Diretiva 95/46/CE, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, ter previsto a sua instituição obrigatória em todos os Estados-Membros. A CNPD, na altura designada como "Comissão Nacional de Proteção de Dados Pessoais Informatizados", foi também criada em momento anterior à Diretiva 95/46/CE pelo art. 4.º, n.º 1, da Lei n.º 10/91, de 29 de abril.

[24] A dificuldade deste exercício de ponderação foi reconhecida pelo Tribunal de Justiça no acórdão de 24 de setembro de 2017, *CNIL*, C-507/17, ECLI:EU:C:2019:772, para. 67: "(...) o interesse do público em aceder a uma informação pode, mesmo dentro da União, variar de um Estado-Membro para outro, pelo que o resultado da ponderação a efetuar entre este, por um lado, e os direitos ao respeito pela vida privada e à proteção dos dados pessoais da pessoa em causa, por outro, não é forçosamente idêntico em todos os Estados-Membros".

As administrações nacionais têm, como corolário do princípio da cooperação leal[25], o dever de assegurar a "execução efetiva" do direito da União (arts. 197, n.º 1, e 291.º, n.º 1, TFUE), atuando funcionalmente como "administração comum da União"[26]. Por esta razão, dir-se-ia, à primeira vista, que a CNPD seria mais um exemplo de autoridade administrativa independente criada ao abrigo do art. 267.º, n.º 3, da Constituição, a quem compete desempenhar o duplo papel de administração nacional e da União.

A natureza jurídica da CNPD distingue-se das restantes entidades administrativas independentes em virtude da sua instituição resultar diretamente do direito primário da União enquanto parte integrante fundamental do direito à proteção de dados – tanto o TFUE (art. 16.º, n.º 2) como a Carta (art. 8.º, n.º 2) referem que o cumprimento da regras relativas à proteção de dados pessoais está sujeita a fiscalização por uma autoridade independente –, e de as suas atribuições e competências estarem previstas no direito secundário (arts. 55.º a 59.º RGPD). Acresce a circunstância de fazer parte da "administração europeia compósita"[27], integrando o Comité Europeu para a Proteção de Dados (art. 68.º, n.º 3, RGPD), organismo da União que é também uma autoridade de controlo independente (arts. 68.º, n.º 1, 69.º, n.º 1, e 70.º, n.º 1, al. a), RGPD)[28],

---

[25] Art. 4.º, n.º 3, TUE. De acordo com o Tribunal de Justiça, "em matérias reguladas pelo direito da União (...), as autoridades públicas dos Estados-Membros estão vinculadas pelo princípio da cooperação leal. Por força deste princípio, tomam todas as medidas gerais ou específicas adequadas para garantir a execução das obrigações decorrentes dos Tratados ou resultantes dos atos das instituições da União e abster-se de qualquer medida suscetível de pôr em perigo a realização dos objetivos da União" (acórdão de 7 de novembro de 2013, *UPC Nederlandl,* C-518/11, ECLI:EU:C:2013:709, para. 59).

[26] PEREZ FERNANDES, Sophie, "Administração Pública", in SILVEIRA, Alessandra; CANOTILHO, Mariana e MADEIRA FROUFE, Pedro (coord.), *Direito da União. Elementos de Direito e Políticas da União*, Almedina, 2016, p. 103, ou TAVARES LANCEIRO, Rui, *O Princípio da Cooperação Leal e a Administração. A Europeização do Procedimento de Acto Administrativo*, AAFDL Editora, 2019, pp. 279 e 280.

[27] LIND, Anna-Sara e Reichel, Jane, "Administrating Data Protection – or the Fort Knox of the European Composite Administration", *Critical Quarterly for Administration and Law*, 2014, 1, pp. 46-54.

[28] O Comité Europeu para a Proteção de Dados sucedeu funcionalmente ao Grupo de Trabalho sobre a proteção das pessoas no que diz respeito ao tratamento de dados pessoais instituído pelo art. 29.º da Diretiva 95/46/CE, órgão consultivo independente que cessou

para além de participar nos procedimentos administrativos complexos de cooperação (arts. 60.º a 62.º) e do controlo de coerência (arts. 63.º a 67.º RGPD)[29].

As autoridades de controlo são, com efeito, um "fenómeno único na União Europeia"[30], na medida em que possuem um estatuto híbrido, que resulta de serem entidades que integram a organização administrativa nacional e simultaneamente exercerem atribuições semelhantes às de uma agência europeia[31].

2.2. A "total independência" das autoridades de controlo

I. De acordo com a jurisprudência constante do Tribunal de Justiça, a instituição nos Estados-Membros de autoridades de controlo independentes constitui um elemento essencial da proteção das pessoas singulares no que respeita ao tratamento dos seus dados pessoais[32]. A garantia de

---

funções com o início de aplicação do RGPD. Inclui como membros um representante – que será, por regra, o respetivo diretor – das autoridades de controlo e a Autoridade Europeia de Proteção de Dados (art. 68.º, n.º 3, RGPD), integrando também nas suas atividades e reuniões representantes da Comissão Europeia (art. 68.º, n.º 5, RGPD). De modo a assegurar a aplicação uniforme do direito da União (e a impedir situações de *forum shopping*), o RGPD atribui-lhe competência decisória vinculativa nos casos previstos nas als. a) a c) do art. 65.º. O Comité Europeu para a Proteção de Dados institucionaliza uma "cooperação institucional" que se distingue de outras formas de cooperação administrativa na União Europeia de natureza informativa (troca de informações) ou procedimental (procedimentos compostos) (v. SCHMITT-AßMANN, Eberhard, "Introduction: European Composite Administration and the Role of European Administrative Law", in JANSEN, Oswald and SCHÖNDORF-HAUBOLD, Bettina (eds.), *The European Composite Administration*, Intersentia, 2011, p. 5).

[29] Sobre o tema dos procedimentos administrativos complexos de execução do direito da União, v. OTERO, Paulo, *Legalidade e Administração Pública. O Sentido da Vinculação Administrativa à Juridicidade*, Almedina, 2003, pp. 479-482, ou TAVARES LANCEIRO, Rui, *O Princípio da Cooperação Leal e a Administração. A Europeização do Procedimento de Acto Administrativo*, cit., pp. 365 a 386.

[30] HIJMANS, Hielke, *The European Union as a constitutional guardian of internet privacy and data protection*, Universidade de Amesterdão, 2016, p. 288.

[31] Idem, pp. 309-311.

[32] *Comissão c. Alemanha*, C-518/07, cit., para. 23; acórdão de 16 de outubro de 2012, *Comissão c. Áustria*, C-614/10, EU:C:2012:631, para. 37; acórdão de 8 de abril de 2014, *Comissão c. Hungria*, C-288/12, EU:C:2014:237, para. 48. V. também o considerando 117 do RGPD.

independência destas entidades visa assegurar a eficácia e a fiabilidade do controlo do cumprimento do direito à proteção de dados e deve ser interpretada à luz deste objetivo[33].

No exercício das suas funções, as autoridades de controlo devem poder agir de forma objetiva e imparcial. Tal implica estarem salvaguardadas de qualquer influência externa, direta ou indireta, oriunda tanto dos organismos controlados como do Estado[34]. No atual contexto de globalização económica e de evolução tecnológica, só assim se evitará o risco de as autoridades de controlo serem capturadas pelo interesse de grandes empresas de tecnologia e dos Estados no acesso indiscriminado a dados pessoais.

Para o tribunal do Luxemburgo, a independência das autoridades de controlo deve ser completa: não é admissível qualquer influência exercida por organismos de tutela ou qualquer instrução ou qualquer outra influência externa que possam pôr em causa o cumprimento da sua tarefa de estabelecer um justo equilíbrio entre a proteção do direito à vida privada e a livre circulação de dados pessoais[35]. Esta ponderação, que deve incluir também outros direitos fundamentais e interesses gerais, constitui uma atribuição fundamental das autoridades de controlo, que requer o exercício de um amplo poder discricionário de apreciação em domínios com grande complexidade técnica e, frequentemente, também de elevada sensibilidade política[36]. O simples risco de que um órgão político de tutela possa influenciar decisões das autoridades de controlo é, por si só, suficiente para impedir o exercício independente das suas funções[37].

O conceito de independência das autoridades de controlo não corresponde sequer ao exigente critério jurisprudencial de independência

---

[33] *Comissão c. Alemanha*, C-518/07, cit., paras. 19 e 25. Neste sentido, v. também a Comunicação da Comissão ao Parlamento Europeu e ao Conselho, *Sobre o acompanhamento do programa de trabalho para uma melhor aplicação da diretiva relativa à proteção de dados*, de 7 de março de 2007, COM(2007) 87 final, p. 7 ["(...) qualquer falha a nível da (...) independência e competência (das autoridades de controlo) tem um impacto negativo considerável quanto ao respeito da legislação em matéria de proteção dos dados"].

[34] Tribunal de Justiça, *Comissão c. Alemanha*, C-518/07, cit., paras. 19 e 25.

[35] Idem, para. 30.

[36] HIJMANS, Hielke, *The European Union as a constitutional guardian of internet privacy and data protection*, Universidade de Amesterdão, 2016, pp. 315-316 e 330-331.

[37] Tribunal de Justiça, *Comissão c. Alemanha*, C-518/07, cit., para. 36.

das entidades a quem é reconhecida a capacidade para suscitar questões prejudiciais ao Tribunal de Justiça[38], podendo inclusivamente dar-se o caso "em que uma autoridade nacional poderia ser considerada suficientemente independente para ser o órgão jurisdicional na aceção do artigo 267.º TFUE, mas, ao mesmo tempo, como não sendo suficientemente independente para ser a autoridade de controlo na aceção (do art. 16.º, n.º 1, TFUE e do art. 8.º, n.º 2, da Carta)"[39].

II. A jurisprudência do Tribunal de Justiça encontrou amplo respaldo no RGPD, que requer que as autoridades de controlo atuem com "total independência" (art. 51.º, n.º 1), não podendo os seus membros estar "sujeitos a influências externas, diretas ou indiretas" ou solicitar ou receber instruções de outrem (art. 51.º, n.º 2), e devendo abster-se de qualquer ato incompatível com as suas funções, não podendo durante o seu mandato desempenhar nenhuma atividade, remunerada ou não, que com elas seja incompatível (art. 51.º, n.º 3)[40].

A ideia, subjacente às declarações do Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República, de que a CNPD não poderia adotar a decisão de desaplicação da lei de execução sem consultar previamente o parlamento constitui uma violação do estatuto de "total independência" da autoridade de controlo

---

[38] Tribunal de Justiça, *Comissão c. Áustria*, C-614/10, cit., para. 40. Sobre o conceito de independência de um "órgão jurisdiciona" na aceção do artigo 267.º TFUE, v. PEREIRA COUTINHO, Francisco, *Os Tribunais Nacionais na Ordem Jurídica da União Europeia: o Caso Português*, Almedina, 2013, pp. 70-78.

[39] Advogado-Geral Ján Mazák, conclusões de 3 de julho de 2012, *Comissão c. Áustria*, C-614/10, ECLI:EU:C:2012:406, para. 25 (nota de rodapé 10). Contra, BALTHASAR, Alexander, "«Complete Independence» of National Data Protection Supervisory Authorities – Second Try: Comments on the Judgment of the CJEU of 16 October 2012, C-614/10 (European Commission v. Austria), with Due Regard to its Previous Judgment of 9 March 2010, C-518/07 (European Commission v. Germany)", *Utrecht Law Journal*, 9, 3, 2013, p. 30, considerando inconcebível admitir a possibilidade de as autoridades de controlo possuírem um grau de independência superior aos tribunais competentes para conhecer recursos das suas decisões.

[40] O estatuto de "total independência" das autoridades de controlo está também previsto no art. 15.º da Convenção Modernizada do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção n.º 108 modificada pelo Protocolo de Alteração), adotada durante a 128.ª sessão do Comité de Ministros do Conselho da Europa, a 18 de maio de 2018 (CM/Del/Dec(2018)128/5).

portuguesa, que impede que esta esteja sujeita a influências externas ou que solicite instruções de outrem no seu processo decisório (art. 51.º, n.º 2, RGPD). Por sua vez, a sugestão de que a Assembleia da República poderia vir a demitir a CNPD em resultado da sua decisão configura uma violação do estatuto de inamovibilidade dos seus membros previsto no RGPD (art. 53.º, n.º 4, RGPD) e na lei de organização e funcionamento da CNPD (art. 5.º, n.º 1, da Lei n.º 43/2004).

O estatuto de "total independência" da CNPD não prejudica a sua sujeição a mecanismos de responsabilização democrática, financeira e judicial (considerando 118 RGPD).

2.3. Meios de responsabilização das autoridades de controlo

I. Uma possível explicação para as declarações do Presidente da 1.ª comissão parlamentar pode estar relacionada com a circunstância de a CNPD funcionar junto da Assembleia da República (art. 2.º, n.º 1, da Lei n.º 43/2004), cujo orçamento financia, quase na totalidade, o seu funcionamento. A Assembleia da República participa também na escolha da CNPD, designando o seu presidente e dois vogais, juntamente com o governo (dois vogais) e os Conselhos Superiores da Magistratura e do Ministério Público (dois vogais) (art. 3.º, n.º 1, da Lei n.º 43/2004).

Uma vez que o processo de designação das autoridades de controlo constitui um fator suscetível de afetar a sua independência, o art. 53.º RGPD impõe um conjunto de condições gerais aplicáveis aos membros das autoridades de controlo que limitam a autonomia processual dos Estados-Membros neste domínio. Esta condições foram cumpridas pelo legislador português que, para além de requerer que os membros da CNPD tenham "integridade e mérito reconhecidos"[41], faz intervir instituições representativas dos três poderes do Estado no seu processo

[41] Proémio do art. 3.º, n.º 1, da Lei n.º 43/2004. Esta disposição deve ser interpretada em conformidade com o art. 53.º, n.º 2, RGPD, que dispõe que os membros das autoridades de controlo devem possuir "as habilitações, a experiência e os conhecimentos técnicos necessários, nomeadamente no domínio da proteção de dados pessoais, ao desempenho das suas funções e ao exercício dos seus poderes".

de designação[42]. Esta é uma solução que, ao mesmo tempo que legitima democraticamente a CNPD, fortalece a sua independência, neutralizando o efeito da participação individual de órgãos de tutela na seleção dos seus membros.

II. A "total independência" das autoridades de controlo determina a impossibilidade de sujeição das mesmas a qualquer espécie de controlo parlamentar da sua atividade. Os Estados-Membros devem garantir que as autoridades de controlo dispõem de orçamentos anuais separados e públicos, os quais podem estar integrados no orçamento geral do Estado[43]. O único mecanismo de responsabilização democrática admitido pelo RGPD consiste na elaboração de um relatório anual de atividades, que deve ser apresentado ao parlamento e ao governo, ao mesmo tempo que é disponibilizado ao público, à Comissão Europeia e ao Comité Europeu de Proteção de Dados[44].

As autoridades de controlo estão, por outro lado, sujeitas à aplicação do direito do Estado-Membro que não afete a sua independência, designadamente as regras relativas ao controlo financeiro da sua atividade (art. 52.º, n.º 6, RGPD).

III. A independência das autoridades de controlo face ao poder político tem como contrapartida necessária a sujeição das suas decisões a controlo jurisdicional. Nos termos do art. 79.º, n.º 1, RGPD: "todas as pessoas singulares ou coletivas têm direito à ação judicial contra as decisões juridicamente vinculativas das autoridades de controlo que lhes digam respeito".

---

[42] O art. 53.º, n.º 1, RGPD exige que os membros das autoridades de controlo sejam nomeados através de um processo transparente, deixando depois aos Estados-Membros a possibilidade de escolha sobre se a designação é feita pelo parlamento, pelo governo, pelo chefe de Estado ou por um organismo independente encarregado da nomeação.

[43] Art. 52.º, n.º 6, RGPD. A Lei n.º 43/2004 reconhece à CNPD autonomia financeira (art. 2.º, n.º 2) e prevê a elaboração de um orçamento anual (art. 20.º, n.º 1).

[44] Art. 59.º RGPD. Está assim ultrapassada a crítica de GARCIA MARQUES e MARTINS, Lourenço, *Direito da Informática*, 2.ª Edição, Almedina, 2006, pp. 365, à ausência de destinatários do relatório anual de atividades da CNPD, cuja elaboração estava prevista no art. 23.º, n.º 1, al. p), da Lei n.º 67/98, de 26 de outubro.

2.4. Independência na prática: o exercício do "mandato Costanzo*"*

I. Na origem das declarações do Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República esteve a decisão da CNPD que recusou a aplicação de diversas normas da lei que procede à implementação do RGPD na ordem jurídica portuguesa com fundamento na sua manifesta incompatibilidade com o direito da União[45]. Apesar de reconhecer a existência de um "direito à resistência" à lei nacional, quando esta contraria o direito europeu, Bacelar de Vasconcelos considerou tal recusa "inadmissível" porque esse direito não pode ser invocado pela CNPD, a qual "não é propriamente um cidadão desprotegido, mas sim um órgão de autoridade de Estado, que foi constituído por via democrática, pelo Parlamento"[46].

Estas críticas não têm razão de ser; a decisão da CNPD merece aplauso, constituindo um exemplo de escola do exercício do "mandato *Costanzo*".

II. O RGPD é um regulamento "obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros" (art. 288.º TFUE). A aplicabilidade direta significa que a sua entrada em vigor e aplicação é "independente de qualquer medida de receção para o direito nacional"[47]. Os Estados-Membros estão, por isso, sujeitos ao dever de não obstruir a aplicabilidade direta do RGPD, designadamente copiando o seu texto para o direito interno quando tal não é necessário à luz dos critérios previstos na jurisprudência, ou interpretando-o ou acrescentando condições adicionais a regras diretamente aplicáveis ao abrigo do regulamento[48]. O cumprimento desta obrigação de não obstrução constitui condição indispensável para a aplicação uniforme do direito da União[49].

---

[45] Deliberação n.º 494/2019, cit., pp. 2-11.

[46] SÉNECA, Hugo, "Parlamento admite que CNPD tem legitimidade para não aplicar lei da proteção de dados. No PS, fala-se em demissão", cit..

[47] Tribunal de Justiça, acórdão de 10 de outubro de 1973, 34/73, *Fratelli Variola*, ECLI:EU:C:1973:101, para. 10.

[48] Comunicação da Comissão ao Parlamento Europeu e ao Conselho, *Maior proteção, novas oportunidades – Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018*, de 24 de janeiro de 2018, COM(2018) 43 final, p. 10.

[49] Tribunal de Justiça, *Fratelli Variola*, 34/73, cit., para. 10.

A aplicabilidade direta do RGPD não prejudica a necessidade de intervenção legiferante dos Estados-Membros destinada a garantir a sua implementação em vários domínios, por exemplo através da adoção de regras que conciliem o direito à proteção de dados pessoais com o direito à liberdade de expressão e de informação (art. 85.º RGPD) ou com o acesso do público a documentos oficiais (art. 86.º RGPD). Múltiplas disposições do RGPD reconhecem também aos Estados-Membros alguma margem de conformação normativa[50], que lhes permite manter ou adotar legislação específica (*v.g.* art. 6.º, n.º 2, RGPD), e, inclusivamente, manter ou acrescentar condições, ou mesmo limitações, à aplicação de regras previstas no RGPD (*v.g.* art. 9.º, n.º 4, RGPD). Uma vez que qualquer ato legislativo nacional adotado neste âmbito se destina a aplicar o direito da União (art. 51.º da Carta), tem necessariamente de respeitar o direito primário, em particular o art. 16.º TFUE e o art. 8.º da Carta dos Direitos Fundamentais da União Europeia.

Sempre que autorizados a introduzir especificações ou restrições a regras previstas no RGPD, os Estados-Membros podem transpor elementos do RGPD para o direito nacional, mas apenas "na medida do necessário para manter a coerência e tornar as disposições nacionais compreensíveis para as pessoas a quem se aplicam" (Considerando 8 do RGPD). A reprodução textual do regulamento deve assim ser algo excecional, não podendo ser utilizada para acrescentar condições ou interpretações adicionais ao articulado do regulamento[51].

A CNPD identificou várias normas da lei de execução que constituem um obstáculo à aplicabilidade direta do RGPD: i) a definição do âmbito territorial de aplicação da lei de execução prevista no seu art. 2.º, n.ºs 1 e 2, compromete a aplicação das normas procedimentais e de distribuição de competência entre as autoridades de controlo dos Estados-Membros previstas no RGPD, sempre que em causa esteja um

---

[50] VOIGT, Paul e von dem BUSSCHE, Axel, *The EU Data Protection Regulation (GDPR). A Practical Guide*, Springer, 2017, pp. 220-222 (Tabela 8.1.).

[51] Comunicação da Comissão ao Parlamento Europeu e ao Conselho, *Maior proteção, novas oportunidades – Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018*, cit., p. 10.

tratamento transfronteiriço[52]; ii) a exclusão dos direitos de informação e de acesso quando a lei imponha ao responsável pelo tratamento ou ao subcontratante um dever de segredo que seja oponível ao próprio titular dos dados prevista no art. 20.º, n.º 1, da lei de execução não respeita o art. 23.º do RGPD, ao não especificar a(s) finalidade(s) que visa salvaguardar e ao não cumprir as exigências previstas no n.º 2 do art. 23.º do RGPD; iii) a faculdade genérica reconhecida no art. 23.º da lei de execução à administração pública de realizar tratamentos de dados pessoais para finalidades diferentes das que justificam a recolha dos dados contraria o princípio da finalidade (art. 5.º, n.º 1, al. b), RGPD) e não cumpre os requisitos impostos para a reutilização de dados previsto no n.º 4 do art. 6.º RGPD; iv) a determinação de que o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador [art. 28.º, n.º 3, al. a), da lei de execução] restringe o âmbito de aplicação da al. a) do n.º 1 do art. 6.º e da al. a) do n.º 2 do art. 9.º RGPD; v) vários aspetos do regime das contraordenações previsto nos arts. 37.º, 38.º e 39.º da lei de execução violam o enquadramento sancionatório previsto no RGPD; vi) a relação de condicionalidade entre o consentimento e a execução de um contrato enquanto fundamentos de licitude autónomos para o tratamento de dados resultante do art. 61.º, n.º 2, da lei de execução é incompatível com a al. 11) do art. 4.º e as als. a) e b) do art. 6.º RGPD; vii) a previsão de que as normas que prevejam autorizações ou notificações de tratamento de dados à CNPD deixam de vigorar à data de entrada em vigor do RGPD (art. 62.º da lei de execução) determina a aplicação retroativa do regulamento, violando o n.º 2 do art. 99.º RGPD.

Em consequência, de forma a assegurar o princípio do primado e a plena efetividade do RGPD, e uma vez não ser possível levar a cabo uma interpretação conforme ao direito da União[53], a CNPD deliberou que, nas

---

[52] Contra, MENEZES CORDEIRO, A. B., "Portugal: A Brief Overview of the GDPR Implementation", cit., p. 536, considerando que o art. 2.º, n.º 1, da lei de execução consubstancia uma norma espacialmente autolimitada que se limita a definir o âmbito de aplicação da lei de execução portuguesa, não afetando o funcionamento do mecanismo do "balcão único" (*one-stop shop*).

[53] À luz do princípio da cooperação leal, a decisão de desaplicação de normas nacionais conflituantes com o direito da União é uma solução de último recurso, a utilizar apenas

situações de tratamento de dados pessoais que seja chamada a apreciar, iria dar prevalência à aplicação das normas do RGPD sobre as normas da lei de execução que manifestamente as contrariam, restringem ou comprometem no seu efeito útil[54].

III. A CNPD fundou a decisão de desaplicação de várias normas da lei de execução no princípio constitucional do primado do direito da União, invocando para o efeito o célebre acórdão *Costa v. Enel*, em que o Tribunal de Justiça declarou que o valor "obrigatório" e a "aplicabilidade direta" dos regulamentos em todos os Estados-Membros prevista no art. 288.º TFUE "seria destituída de significado se um Estado pudesse, unilateralmente, anular os seus efeitos através de um ato legislativo oponível aos textos (da União)"[55].

Um dos principais corolários da doutrina do primado, conjugada com o princípio da cooperação leal, é o chamado "mandato *Costanzo*": todas as instâncias de um Estado-Membro encarregadas de aplicar, no âmbito das respetivas competências, as disposições do direito da União têm a obrigação de garantir a plena eficácia dessas disposições, não aplicando, se necessário, no exercício da sua própria autoridade, qualquer disposição nacional contrária, sem pedir ou aguardar pela eliminação prévia dessa disposição ou por qualquer outro procedimento constitucional[56].

---

depois de se verificar que não ocorre antinomia aparente que pode ser resolvida através da interpretação das normas internas em conformidade com o direito da União (Tribunal de Justiça, acórdão de 22 de dezembro de 2010, *Rosa María Gaviero Gaviero*, C-444/09 e C-456/09, ECLI:UE:C:2010:819, para. 73). Sobre este tema, v. VERHOEVEN, Maartje, "The «Costanzo Obligation» of National Administrative Authorities in the Light of the Principle of Legality: Prodigy or Problem Child?", *Croatian Yearbook of European Law and Policy*, 5, 2009, pp. 67-69.

[54] Deliberação n.º 494/2019, cit., pp. 3-11.

[55] Acórdão de 15 de julho de 1964, *Costa v. Enel*, 6/64, ECLI:EU:C:1964:66, p. 556.

[56] Tribunal de Justiça, C-378/17, acórdão de 4 de dezembro de 2018, *Minister for Justice and Equality*, ECLI:EU:C:2018:979, para. 35, 38 e 39. Esta obrigação foi reconhecida pelo Tribunal de Justiça, em relação aos tribunais nacionais, no acórdão de 9 de março de 1978, *Simmenthal*, 106/77, ECLI:EU:C:1978:49, para. 22, e, em relação aos restantes órgãos do Estado, incluindo as autoridades administrativas, no acórdão de 22 de junho de 1989, *Costanzo*, 103/88, ECLI:EU:C:1989:256, para. 31. Sobre o alcance do "mandato ou obrigação *Costanzo*", v. CLAES, Monica, *The National Courts' Mandate in the European Constitution*, Hart, 2006, pp. 266-278; VERHOEVEN, M. J. M., *The Costanzo Obligation: The Obligations of National Administrative Authorities in the Case of Incompatibility Between National Law and European Law*, Intersentia, 2011,

As autoridades administrativas têm assim o dever de superar antinomias normativas desaplicando o direito nacional conflituante com o direito da União, ainda que o princípio da separação de poderes lhes proscreva o poder de apreciar a legalidade de normas de direito interno[57]. Esta é uma decisão que comporta riscos para a aplicação uniforme do direito da União, em virtude de ter de ser tomada sem a possibilidade de pedir a intervenção a título prejudicial do Tribunal de Justiça ao abrigo do mecanismo das questões prejudiciais previsto no art. 267.º TJUE[58].

IV. A CNPD é o órgão criado para dar cumprimento à obrigação que recai sobre o Estado português de estabelecer uma autoridade de controlo nacional (art. 51.º, n.º 1, RGPD).

Enquanto órgão competente para controlar e executar a aplicação do RGPD no território português (arts. 55.º e 57.º, n.º 1, al. a), RGPD) e para contribuir para a sua "aplicação coerente" em toda a União (art. 51.º, n.º 2, RGPD), a CNPD tem, por força dos princípios da cooperação leal e do primado do direito da União, a obrigação de assegurar, no âmbito do exercício dessas competências, o pleno efeito desse direito, não aplicando, se necessário, qualquer disposição eventualmente contrária da lei nacional[59].

Sempre que chamada a pronunciar-se sobre um litígio no quadro de um processo de reclamação (arts. 57.º, al. f), e 77.º, n.º 1, RGPD), a

---

e TAVARES LANCEIRO, Rui, *O Princípio da Cooperação Leal e a Administração. A Europeização do Procedimento de Acto Administrativo*, cit., pp. 304-328.

[57] FRAGOSO MARTINS, Patrícia, *Administrações Públicas Nacionais e Direito da União Europeia. Questões e Jurisprudência Essenciais*, Universidade Católica Editora, 2018, p. 84, refere, a este propósito, que "a jurisprudência europeia parece convidar ou impor a necessidade de repensar os fundamentos, sentido e alcance do princípio nacional da legalidade, na sua dupla vertente de precedência da lei e de prevalência da lei". Como bem nota TAVARES LANCEIRO, Rui, *O Princípio da Cooperação Leal e a Administração. A Europeização do Procedimento de Acto Administrativo*, cit., p. 320, a jurisprudência *Costanzo* obriga à rejeição da "visão do princípio da legalidade que apenas equaciona a lei nacional, pois (esta) esquece que o direito da (União) integra, atualmente, o bloco de legalidade vinculativo da administração".

[58] DE WITTE, Bruno, "Direct Effect, Supremacy and the Nature of the Legal Order", in CRAIG, Paul e DE BÚRCA, Gráinne, *The Evolution of EU Law*, 2.ª Edição, Oxford University Press, 2011, p. 333.

[59] Tribunal de Justiça, *Minister for Justice and Equality*, C-378/17, cit., para. 45.

intervenção da CNPD visa também assegurar a proteção jurídica que o direito da União confere aos titulares dos dados. Neste contexto, seria contraditório que estes pudessem invocar as disposições do direito da União num domínio específico perante o órgão a quem o direito nacional atribuiu a competência para dirimir litígios no domínio do direito da proteção de dados e que o referido órgão não tivesse a obrigação de aplicar aquelas disposições, afastando as de direito nacional que as contrariassem[60]. Acresce que, na eventualidade de a CNPD ser qualificada como um "órgão jurisdicional" na aceção do art. 267.º (2) TFUE, pode submeter ao Tribunal de Justiça questões prejudiciais que envolvam a interpretação ou a apreciação de validade de disposições de direito da União nos litígios que seja chamada a resolver; uma vez que está vinculada pelo acórdão proferido a título prejudicial pelo Tribunal de Justiça, deve dar imediatamente cumprimento ao mesmo, não aplicando, se necessário e no exercício da sua própria autoridade, as disposições contrárias da legislação nacional[61].

V. Mas podem as autoridades de controlo nacionais remeter reenvios prejudiciais para o Tribunal de Justiça?

A apreciação da competência para apresentar pedidos prejudiciais é uma questão que releva unicamente do direito da União[62]. A questão de saber se a entidade responsável pelo reenvio tem a natureza de órgão jurisdicional na aceção do artigo 267.º TFUE é apreciada pelo Tribunal de Justiça com base num conjunto de elementos, como a origem legal do órgão, o caráter obrigatório e permanente da sua jurisdição, a natureza contraditória do processo, a aplicação, pelo órgão, de regras de direito, bem como a sua independência[63]. Para além disso, as entidades nacionais só podem pedir ao Tribunal de Justiça que se pronuncie se perante elas se encontrar pendente um litígio e se forem chamadas a pronunciar-se

---

[60] Tribunal de Justiça, *Costanzo*, 103/88, cit., para. 31.

[61] *Minister for Justice and Equality*, C-378/17, cit., para. 47.

[62] Advogada-Geral Juliane Kokott, conclusões de 20 de setembro de 2012, *Belov*, C-394/11, ECLI:EU:C:2012:585, para. 26.

[63] Acórdão de 27 de fevereiro de 2018, *Associação Sindical dos Juízes Portugueses*, C-64/16, EU:C:2018:117, para. 28.

no âmbito de um processo que deva conduzir a uma decisão de caráter jurisdicional[64].

No processo *Comissão c. Áustria*, o governo austríaco argumentou que o Tribunal de Justiça, no acórdão *Dorsch Consult*[65], aceitou responder a questões prejudiciais suscitadas por entidade com uma natureza semelhante à comissão de proteção de dados austríaca[66].

À luz das garantias de autonomia e imparcialidade previstas no RGPD, não restam dúvidas sobre o preenchimento pelas autoridades de controlo nacionais do critério da independência, o qual constitui "a característica de diferenciação mais importante para distinguir entre um órgão jurisdicional nacional e uma autoridade administrativa"[67]. Também é pacífico o preenchimento dos critérios estruturais relativos à origem legal, permanência e aplicação de regras de direito. O mesmo sucede com a natureza contraditória do processo que, não constituindo um critério absoluto[68], se pode considerar satisfeito com a existência de um direito de audiência prévia (*v. g.* o art. 121.º do Código do Procedimento Administrativo), e, finalmente, com o requisito do caráter obrigatório da jurisdição, desde que este critério seja interpretado como dizendo respeito "ao caráter vinculativo das decisões da entidade de reenvio"[69]. No plano funcional, a possibilidade de recurso ao processo do art. 267.º TFUE pressupõe a existência de um litígio, que é inerente a processos de reclamação perante autoridades de controlo, e requer que o órgão de reenvio exerça uma atividade jurisdicional.

O preenchimento do critério funcional relativo ao exercício de uma atividade jurisdicional pelas autoridades de controlo nacionais apresenta-se controvertido após o Tribunal de Justiça se ter pronunciado, no acórdão *Belov*, pela inadmissibilidade do reenvio prejudicial submetido pela comissão de defesa contra a discriminação da Bulgária[70]. O tribunal do

---

[64] Acórdão de 14 de outubro de 1995, *Job Centre*, C-111/94, ECLI:EU:C:1995:340, para. 9.

[65] Acórdão de 17 de setembro de 1997, C-54/96, ECLI:EU:C:1997:41.

[66] Advogado-Geral Ján Mazák, *Comissão c. Áustria*, C-614/10, cit., para. 23.

[67] Advogada-Geral Stix-Hackl, conclusões de 11 de maio de 2006, *Wilson*, C-506/04, ECLI:EU:C:2006:311, para. 45.

[68] C-54/96, *Dorsch Consult*, cit., para. 31.

[69] Advogada-Geral Juliane Kokott, *Belov*, C-394/11, cit., para. 48.

[70] Acórdão de 31 de janeiro de 2013, C-395/11, ECLI:EU:C:2013:48.

Luxemburgo considerou que a decisão que esta entidade era chamada a proferir no âmbito de um processo de reclamação se assemelhava, no essencial, a uma decisão de tipo administrativo e não revestia caráter jurisdicional, em virtude de o órgão de reenvio: i) ter competência para desencadear oficiosamente um processo no essencial semelhante ao que deu origem à reclamação; ii) poder ordenar a intervenção no processo de pessoas diferentes das arroladas pela reclamante; iii) ter a qualidade de recorrida no tribunal administrativo chamado a conhecer do recurso interposto da sua decisão; iv) poder anular a decisão uma vez interposto recurso da sua decisão no processo de reclamação, desde que tenha o acordo da parte a que essa decisão é favorável[71].

A partir da articulação do acórdão *Belov* com o acórdão *Schrems*[72], em que o Tribunal de Justiça não considerou a possibilidade de as autoridades de controlo submeterem reenvios prejudiciais sobre a validade de decisões de adequação da Comissão, pode-se concluir que as autoridades de controlo não podem ser consideradas "órgãos jurisdicionais" na aceção do art. 267.º TFUE[73]. Os riscos para a uniformidade na aplicação do direito da União resultantes desta qualificação são mitigados pelo direito das pessoas singulares e coletivas à ação judicial contra as decisões juridicamente vinculativas das autoridades de controlo que lhes digam respeito (art. 78.º, n.º 1, RGPD). Nos termos do artigo 267.º TFUE, o órgão jurisdicional nacional em que for intentada a ação tem a faculdade ou, se for caso disso, é obrigado a submeter um pedido de decisão prejudicial ao Tribunal de Justiça se for necessária uma decisão sobre a interpretação ou validade do direito da União (Considerando 143 RGPD). Em todo o caso, a circunstância de as autoridades de controlo não constituírem "órgãos jurisdicionais" na aceção do artigo 267.º TFUE obviamente não as "dispensa da obrigação de garantir a aplicação do direito da União aquando da adoção das suas decisões e de não aplicar, se necessário, as disposições nacionais que se revelem contrárias a disposições do direito da União dotadas de um efeito direto, uma vez que tais obrigações vinculam,

---

[71] *Belov*, C-395/11, cit., paras. 46-52.

[72] Acórdão de 6 de outubro de 2015, C-362/14, ECLI:EU:C:2015:650, paras. 64-65.

[73] Neste sentido, MUIR, Elisa, *EU Equality Law: The First Fundamental Rights Policy of the EU*, Oxford University Press, 2018, pp. 190-193.

efetivamente, todas as autoridades nacionais competentes e não apenas as autoridades jurisdicionais"[74].

VI. Poder-se-ia discutir a legitimidade de uma decisão administrativa de desaplicação do direito nacional desconforme com o direito da União com uma natureza prospetiva. O "mandato *Costanzo*" constitui um desenvolvimento do "mandato *Simmenthal*" nos termos do qual se impõe aos órgãos administrativos nacionais a obrigação de atribuição de plena eficácia às normas da União "no âmbito das respetivas competências"[75]. Ora, ao contrário da atividade jurisdicional, o exercício da atividade administrativa não pressupõe sempre a aplicação do direito da União num caso concreto. A CNPD invocou o interesse "de assegurar a transparência dos seus procedimentos decisórios futuros e nesta medida contribuir para a certeza e segurança jurídicas"[76]. Trata-se, com efeito, de entendimento que se esteia no princípio da cooperação leal, contribuindo para a aplicação uniforme do direito da União, que se enquadra perfeitamente nas suas amplas atribuições de controlo e execução da aplicação do RGPD (art. 57.º, n.º 1, al. a), RGPD), bem como de pronuncia não vinculativa sobre medidas legislativas relativas à proteção de dados pessoais (art. 6.º, n.º 1, al. a), da lei da execução).

Apenas se lamenta que a apreciação da compatibilidade da lei de execução com o direito da União não tenha sido exaustiva. A CNPD circunscreveu a sua análise apenas às disposições da lei de execução mais relevantes e de aplicação mais frequente[77]. Acontece que no Parecer n.º 28/2018, de 2 de maio, relativo à proposta de lei de execução, identificou infrações ao direito da União – algumas das quais qualificou como manifestas – em diversas disposições que estão previstas na lei de execução[78].

---

[74] Tribunal de Justiça, acórdão de 21 de janeiro de 2020, *Banco de Santander*, C-274/14, ECLI:EU:C:2020:17, para. 78.

[75] Idem, paras. 38-39.

[76] Deliberação n.º 494/2019, cit., p. 11.

[77] Idem, pp. 1-2.

[78] Entre as quais se inclui o art. 4.º, n.ºs 3 e 4 (natureza e independência), o art. 6.º, al. d) (atribuições e competências), o art. 7.º, n.º 1 (avaliações prévias de impacto), o art. 8.º (dever de colaboração), o art. 11.º (funções do encarregado de proteção de dados), o art. 12.º, n.ºs 3 e 4 (encarregados de proteção de dados em entidades públicas), o art. 13.º (encarregados de proteção de dados em entidades privadas), o art. 14.º, n.ºs 2 e 3 (acreditação e certificação);

Por maioria de razão, à luz do princípio da certeza e da segurança jurídica, e de modo a contribuir para a aplicação uniforme do direito da União, a CNPD tinha a obrigação de indicar todas as normas da lei de execução que considera incompatíveis com o direito da União, não podendo circunscrever a sua apreciação a um juízo de prognose, necessariamente subjetivo, sobre a sua relevância ou a frequência de aplicação.

VII. O exercício pela CNPD do "mandato *Costanzo*" na Deliberação n.º 494/2019, de 3 de setembro, contrasta frontalmente com o que precedeu decisão homóloga de desaplicação da Lei n.º 32/2008, de 17 de julho, que transpôs a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

A 8 de abril de 2014, o Tribunal de Justiça declarou a invalidade da Diretiva 2006/24/CE com fundamento na violação do princípio da proporcionalidade na restrição que a diretiva opera no direito à privacidade e à proteção de dados pessoais consagrados nos arts. 7.º e 8.º da Carta[79]. No final de 2016, o tribunal do Luxemburgo esclareceria não ser admissível a aplicação de legislação nacional que preveja, para efeitos de luta contra a criminalidade, "uma conservação generalizada e indiferenciada de todos os dados de tráfego e de todos os dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica"[80].

A Lei n.º 32/2018, de 17 de julho, obriga os fornecedores de comunicações eletrónicas a operar em Portugal a reter indiscriminadamente, durante um período de um ano, todos os dados de tráfego e de localização de todos os seus clientes, atribuindo à CNPD a competência para instruir

---

o art. 18.º (portabilidade e interoperabilidade dos dados), o art. 21.º (prazo de conservação de dados), art. 22.º (transferências internacionais), art. 26.º (acesso a documentos administrativos), o art. 28.º, n.º 2, n.º 3, al. b) (relações laborais) e o art. 31.º (tratamentos para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos).

[79] Acórdão de 8 de abril de 2014, *Digital Rights Ireland, Ltd*, C-293/12 e C-594/12, ECLI:EU:C:2014:238, para. 69.

[80] Acórdão de 21 de dezembro de 2016, *Tele2*, C –203/15 e C-698/15, ECLI:EU:C:2016:970, para. 112.

processos de contraordenação e aplicar coimas resultantes da violação da obrigação de conservação destes dados pessoais (arts. 4.º, 6.º, 12.º e 14.º). Uma vez que se trata de lei que implementa direito da União na aceção do art. 51.º, n.º 1, da Carta[81], deve conformar-se com as exigências decorrentes dos direitos fundamentais garantidos na ordem jurídica da União[82]. À luz da jurisprudência *Digital Rights* e *Tele2*, o tratamento generalizado e indiferenciado de dados pessoais que a Lei n.º 32/2008, de 17 de julho, impõe aos fornecedores de comunicações eletrónicas constitui uma ingerência desproporcionada "de grande amplitude e particular gravidade" nos direitos fundamentais à privacidade e à proteção de dados[83]. Esta "evidente incompatibilidade" com o direito da União[84], obriga todos os órgãos do Estado português a recusar a sua aplicação por força do princípio do primado[85].

Como reagiu a CNPD à declaração de invalidade do ato legislativo que foi considerado pela Autoridade Europeia para a Proteção de Dados como o mais invasivo para a privacidade dos cidadãos alguma vez adotado pela União Europeia[86]?

---

[81] Trata-se, com efeito, de uma lei de transposição que, após a cessação de efeitos da diretiva que lhe deu causa, se enquadra no âmbito de aplicação do art. 15.º da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (*Tele2*, C-203/15 e C-698/15, cit., paras. 75-81).

[82] Tribunal de Justiça, acórdão de 26 de fevereiro de 2013, *Fransson,* C-617/10, ECLI:EU:C:2013:105, para. 18.

[83] Tribunal de Justiça, *Digital Rights Ireland, Ltd*, C-293/12 e C-594/12, cit., para. 65.

[84] SILVEIRA, Alessandra e FREITAS, Pedro Miguel, "The Recent Jurisprudence of the CJEU on Personal Data Retention: Implications for Criminal Investigation in Portugal", *UNIO – EU Law Journal*, 3, 2, 2017, p. 53. No mesmo sentido, GUERRA, Clara e CALVÃO, Filipa, "Anotação ao Acórdão do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014", *Forum de proteção de dados*, 1, julho de 2015, p. 81.

[85] SILVA RAMALHO, David e COIMBRA, José Duarte, "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves", *O Direito*, 147, 3, 2015, p. 1040.

[86] HUSTINX, Peter "The Moment of Truth for the Data Retention Directive", Conferência "Taking on the Data Retention Directive", 3 de dezembro de 2010, p. 1 ("A (Diretiva 2006/24/CE) é sem dúvida o instrumento mais invasivo para a privacidade alguma vez adotado pela União Europeia em termos de escala e do número de pessoas que afeta").

Começou por anunciar na Assembleia da República a necessidade de se preceder à "análise" da conformidade da Lei n.º 32/2008, de 17 de julho, com o direito da União à luz do acórdão *Digital Rights* proferido semanas antes[87]. O período de reflexão prolongou-se por mais de três anos: i) a 26 de junho de 2015, em parecer sobre o regime de acesso a metadados pelos serviços de informação, a CNPD deu conta de que a "legitimidade" da base de dados criada pela Lei 32/2008, de 17 de julho, "não está ainda determinada na nossa ordem jurídica"[88]; ii) a 9 de maio de 2017, em parecer sobre iniciativa legislativa com o mesmo objeto, referiu que a desproporcionalidade da recolha indiscriminada de dados "faz perigar (...) a «validade»" da Lei n.º 32/2008, de 17 de julho, à luz da Carta[89]. A reflexão terminou com a conclusão, anunciada em deliberação de 9 maio de 2017, de que "sendo certo que a declaração de invalidade da diretiva não implica diretamente a invalidade da lei nacional que a transponha", os Estados-Membros têm o dever de "reavaliar a conformidade com a Carta dos respetivos regimes nacionais de retenção de dados (...) à luz dos fundamentos expostos (pelo Tribunal de Justiça)", aqui se incluindo também o Estado português, considerando a CNPD ser seu dever "alertar a Assembleia da República para a necessidade de reavaliar a Lei n.º 32/2008, de 17 de julho, em termos de conformidade com a Carta"[90].

---

[87] CALVÃO, Filipa (Presidente da Comissão Nacional de Proteção de Dados), "Audiência sobre o relatório de atividades de 2012 e matérias que estejam no âmbito das suas competências", *Audiência Parlamentar Nº 51-CACDLG-XII*, 29 de abril de 2014, 17:39 a 17:48.

[88] Parecer n.º 51/2015, de 26 de junho, p. 10.

[89] Parecer n.º 24/2017, de 18 de abril, p. 20-21. A qualificação de uma incompatibilidade com o direito da como um problema de validade da lei nacional, ignora a jurisprudência do Tribunal de Justiça, segundo a qual não pode ser deduzido que "a incompatibilidade com o direito da União de uma norma de direito nacional posterior (tenha) por efeito tornar esta norma inexistente. Face a uma tal situação, o órgão jurisdicional nacional está, diferentemente, obrigado a afastar a aplicação da norma (...) (acórdão de 22 de outubro de 1998, *IN.CO.GE.*, C-10/97 a C-22/97, ECLI:EU:C:1998:498, para. 21). Por outras palavras, o princípio do primado tem como efeito a ineficácia e não a invalidade do direito nacional conflituante com o direito da União, decorrendo do princípio da cooperação leal o dever da sua desaplicação por todos os órgãos do Estado, incluindo as autoridades administrativas.

[90] Deliberação n.º 1008/2017, de 18 de julho, pp. 1 e 3.

O "alerta" foi completamente ignorado: a Lei n.º 32/2008, de 17 de julho, permanece em vigor e tem sido regularmente aplicada pelos tribunais[91].

[91] V., por exemplo, o acórdão do Tribunal da Relação de Lisboa de 28 de novembro de 2018, processo 8617/17.8T9LSB-A.L1-3, que obrigou a Vodafone a fornecer dados de tráfego retidos ao abrigo da Lei n.º 32/2008, de 17 de julho, considerando que "a declaração de invalidade da Diretiva 2006/24/CE (...) não tem uma consequência automática sobre a validade do ato legislativo interno que a transpôs, porquanto o ato legislativo nacional tem uma fonte autónoma de validade e legitimidade, pois não se limitou a transpor tal diretiva, antes a densificando e aperfeiçoando ao direito interno, sendo que a análise do Tribunal de Justiça apenas incidiu sobre o texto da diretiva". Este aresto, que manifestamente confunde a vigência formal da Lei n.º 32/2008, de 17 de julho, a qual se afigura pacífica, com o dever de os órgãos jurisdicionais nacionais a desaplicarem em resultado da sua incompatibilidade com a Carta, baseia-se no acórdão do Tribunal Constitucional n.º 420/2017, de 13 de julho, processo n.º 917/16. Decidindo em processo de fiscalização concreta, o Tribunal Constitucional não julgou inconstitucional a norma da Lei n.º 32/2008 que estabelece o dever de os fornecedores de serviços de comunicações eletrónicas conservarem "os dados relativos ao nome e ao endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP estava atribuído no momento da comunicação", considerando que tal norma não viola o princípio da proporcionalidade decorrente do art. 18.º, n.º 2, da Constituição. Esta decisão merece algumas (necessariamente breves) observações. O art. 1.º da Lei n.º 32/2008, de 17 de julho, transpôs o art. 1.º, n.ºs 1 e 2, da Diretiva 2006/24/CE, que requeria aos Estados-Membros a conservação de "dados conexos necessários para identificar o assinante ou o utilizador", entre os quais se incluem o nome e o endereço do assinante ou do utilizador registado a quem o endereço do protocolo IP estava atribuído no momento da comunicação (art. 5.º, n.º 1, 2), da Diretiva 2006/24/CE), enquadrando-se agora no âmbito de aplicação do art. 15.º da Diretiva 2002/58/CE, de 12 de julho. Daqui resulta estarmos perante legislação nacional "inteiramente determinada" pelo direito da União na aceção do acórdão *Fransson* do Tribunal de Justiça (C-617/10, cit., n.° 29), o que significa que o juízo de proporcionalidade da restrição que impõe nos direitos à privacidade e à proteção de dados tinha de ser feito, em primeira linha, à luz da Carta e não da Constituição, cabendo, em última instância, ao Tribunal de Justiça e não, como aconteceu, ao Tribunal Constitucional. Mas ainda que se entenda que se trata de legislação nacional "não inteiramente determinada" pelo direito da União, o que permitiria ao Tribunal Constitucional aplicar os padrões de proteção dos direitos fundamentais previstos na Constituição, em nenhuma circunstância poderia dessa aplicação resultar um nível de proteção menos elevado do que aquele que é garantido pela Carta ou o comprometimento do primado, da unidade ou da efetividade do direito da União (Tribunal de Justiça: *Fransson*, C-617/10, cit., para. 29, ou acórdão de 26 de fevereiro de 2013, *Melloni*, C-399/11, ECLI:EU:C:2013:107, para. 60). Ora, os juízes do Palácio Ratton argumentaram que a desproporcionalidade da retenção indiscriminada de dados assinalada pelo Tribunal de Justiça nos acórdãos *Digital Rights* e *Tele2* diz respeito a dados de tráfego e de localização, mas "não exatamente sobre os dados de base" que estavam em causa neste processo (mas já não

no processo julgado na Relação de Lisboa). Trata-se de uma interpretação muito discutível dos acórdãos *Digital Rights* e *Tele2*, que manifestamente exigia, à luz da jurisprudência *Cilfit* (acórdão de 6 de outubro de 1982, 283/81, ECLI:EU:C:1982:335, para. 16), a suscitação de uma questão prejudicial ao abrigo do art. 267.º do TFUE sobre a conformidade com a Carta da conservação indiscriminada de "dados de base ou de rede". É que o acesso aos dados pessoais dos assinantes levanta questões de privacidade que não podem ser comparadas à consulta de "uma lista telefónica tradicional ou de uma base dados pública de matrículas de automóveis", pois "de forma a identificar o assinante a quem foram atribuídos endereços específicos de IP dinâmicos, o fornecedor de serviços de telecomunicações tem de aceder a dados retidos que dizem respeito a determinadas atividades de telecomunicação" (Tribunal Europeu dos Direitos Humanos, queixa n.º 62357/14, acórdão de 14 de abril de 2018, *Benedik c. Eslovénia*, para. 108). A natureza controvertida desta questão foi também recentemente assinalada pelo Conselho, *Draft Council Conclusions on Improving Retention of Data for the Purpose of Fighting Crime Effectively*, de 27 de março de 2019, 7833/19, p. 2 ["(...) *tem sido argumentado* que as decisões do (Tribunal de Justiça nos acórdãos *Digital Rights* e *Tele2*) se aplicam apenas a dados de tráfico e de localização, e não aos dados dos assinantes" (itálico acrescentado)]. No acórdão n.º 494/2019, de 18 de setembro, processo n.º 26/2018, o Tribunal Constitucional perderia nova oportunidade para participar, pela primeira vez na sua história, no diálogo jurisprudencial que continuamente alimenta a evolução do direito da União Europeia; uma questão prejudicial sobre a conformidade com a Carta de legislação nacional que prevê uma obrigação geral de conservação de dados com o objetivo de proteger a segurança nacional, a defesa do território e a segurança pública – similar à colocada pelo Tribunal Constitucional belga no processo C-520/18 (*Ordre des barreaux francophones and germanophone*) – não foi sequer considerada porque se concluiu que, uma vez que a Lei Orgânica n.º 4/2017, de 25 de agosto, regula apenas o acesso a metadados pelos serviços de informações, não era necessária pronuncia sobre a validade da Lei n.º 32/2008, de 17 de julho, não obstante parecer claro que o efeito útil da apreciação de constitucionalidade está necessariamente comprometido se a lei que permite a conservação dos dados transmitidos aos serviços de informações não puder ser aplicada por ser desconforme ao direito da União. Não se compreende, por último, a referência feita pelo Tribunal Constitucional no acórdão n.º 420/2017, de 13 de julho – e, influenciado por este, também pelo Tribunal da Relação de Lisboa – à Nota Prática do Ministério Público n.º 7/2015, de 30 de dezembro, "Retenção de Dados de Tráfego e Lei n.º 32/2008, de 17 de julho". Esta nota é um instrumento não vinculativo elaborado pelo gabinete de cibercrime da Procuradoria Geral da República que, baseando-se no argumento de que o resultado de um conflito normativo entre fontes nacionais e europeias não tem como efeito a invalidade do direito interno, exorta à aplicação da Lei n.º 32/2008, de 17 de julho, concluindo, numa deriva securitária orwelliana não suficientemente fundamentada e abertamente contrária à jurisprudência do Tribunal de Justiça, que "a retenção de dados tem que ser indiscriminada, por um lado, e tem que abranger todos os cidadãos, por outro". Para uma crítica a esta nota prática,

O princípio do primado impunha à CNPD a adoção das medidas necessárias para garantir a plena eficácia do direito da União, o que implicava recusar a aplicação da Lei n.º 32/2008, de 17 de julho, logo após a prolação do acórdão *Digital Rights*[92]. À autoridade administrativa especificamente mandatada para afastar legislação nacional que contrarie direito da União relativo à proteção de dados não lhe cabia pedir – essa é a prerrogativa, designadamente, do Provedor de Justiça[93] – ou aguardar pela eliminação prévia da Lei n.º 32/2008, de 17 de julho, "por via legislativa ou por qualquer outro procedimento constitucional"[94]. Não se afigura, por isso, aceitável que o anúncio da desaplicação da Lei n.º 32/2008, de 17

---

v. SILVEIRA, Alessandra e FREITAS, Pedro Miguel, "Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos Estados-Membros da UE: uma leitura jusfundamental", *Revista de Direito Setorial e Regulatório*, 3, 1, 2017, pp. 291-293.

[92] A decisão do Tribunal de Justiça que declara a invalidade num processo prejudicial produz, na prática, efeitos *erga omnes*, projetando-se sobre todos os órgãos jurisdicionais, legislativos e administrativos (SILVA RAMALHO, David e DUARTE COIMBRA, José , "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves", cit., p. 1022).

[93] Nos termos da al. b), n.º 1, do art. 20.º do Estatuto do Provedor de Justiça (Lei n.º 9/91, de 9 de abril), ao Provedor de Justiça compete "assinalar as deficiências de legislação que verificar, emitindo recomendações para a sua interpretação, alteração ou revogação". Foi esse o propósito da Recomendação n.º 1/B/2019, de 22 de janeiro, em que se solicita à Ministra da Justiça a alteração da Lei n.º 32/2008, de 17 de julho, de modo a que o seu regime se adeque "com as exigências decorrentes da Carta dos Direitos Fundamentais da União Europeia, tal como foram interpretadas pela jurisprudência pertinente do Tribunal de Justiça". Em ofício de 4 de março de 2019, a Ministra da Justiça recusou iniciar um processo legislativo com este propósito junto da Assembleia da República, invocando a complexidade da matéria e a circunstância de a lei portuguesa "parece(r) assegurar, apesar de tudo medidas proporcionais suficientes entre os direitos conflituantes da intimidade da vida privada e da proteção dos dados pessoais, pelo que a decisão do TJUE (*Digital Rights*) não deverá afetar as investigações nacionais (sic), em conformidade com o Acórdão do Tribunal Constitucional n.º 490/2017, de 13 de julho". A 26 de agosto de 2019, a Provedora de Justiça solicitou, ao abrigo do disposto no art. 281.º, al. a), e n.º 2, al. d), da Constituição, a fiscalização abstrata da constitucionalidade dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de julho, por violação do princípio da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada e familiar (art. 26.º, n.º 1) e ao sigilo das comunicações (art. 34.º, n.º 1) e por violação do direito a uma tutela jurisdicional efetiva (art. 20.º, n.º 1).

[94] Tribunal de Justiça, *Minister for Justice and Equality*, C-378/17, cit., para. 50.

de julho, tenha surgido apenas em deliberação de 18 de julho de 2017[95], mais de 39 meses depois do acórdão *Digital Rights*!

A decisão de desaplicação da lei de execução menos de um mês depois da sua entrada em vigor parece significar que a CNPD não vai doravante tergiversar na sua missão de fiscalização do cumprimento do RGPD na ordem jurídica portuguesa. Ironicamente, o exercício efetivo deste papel depende, em larga medida, dos recursos de que venha a ser provida pela Assembleia da República.

3. Os recursos das autoridades de controlo

3.1. Independência e efetividade

A criação de autoridades de controlo totalmente independentes em cada Estado-Membro constitui condição necessária, mas não suficiente, para assegurar a eficácia do controlo do cumprimento do direito à proteção de dados. O RGPD impõe aos Estados-Membros o dever de assegurar "que cada autoridade de controlo disponha dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessários à prossecução eficaz das suas atribuições e ao exercício dos seus poderes, incluindo as executadas no contexto da assistência mútua, da cooperação e da participação no Comité" (art. 52.º, n.º 4).

O princípio da efetividade do direito da União requer que os Estados-Membros forneçam às autoridades de controlo os meios necessários ao cumprimento das suas atribuições[96], que incluem lidar eficazmente com reclamações dos titulares dos dados, realizar investigações eficazes, tomar decisões vinculativas e impor sanções dissuasoras aos responsáveis pelo

---

[95] Deliberação n.º 1008/2017, de 18 de julho, cit., p. 3, a qual também teve, à semelhança da Deliberação n.º 494/2019, de 3 de setembro, uma natureza prospetiva, não obstante a CNPD ter referido a receção de "participações do Ministério Público de diversas comarcas por eventual incumprimento da Lei n.º 32/2008, por parte de diversas operadoras de telecomunicações".

[96] HIJMANS, Hielke, *The European Union as a constitutional guardian of internet privacy and data protection*, Universidade de Amesterdão, 2016, p. 322.

tratamento ou aos subcontratantes[97]. O cumprimento desta obrigação é, por outro lado, crucial para assegurar a aplicação uniforme do RGPD, pois o mau funcionamento de uma autoridade de controlo resultante da situação de subfinanciamento pode colocar em causa procedimentos administrativos complexos que integram autoridades de controlo de outros Estados-Membros.

3.2. Os recursos da CNPD

I. Num relatório de 2010 da Agência Europeia para a Proteção dos Direitos Fundamentais (FRA), a CNPD surge identificada, a par das suas congéneres na Áustria, Bulgária, Eslováquia, Roménia, Chipre, França, Grécia, Holanda, Itália e Letónia, como uma das autoridades de controlo que não está "em condições de exercer na plenitude as suas atribuições em razão dos limitados recursos económicos e humanos de que (dispõe)"[98]. Estas lacunas foram também identificadas pela Comissão em 2012[99], que as invocou como uma das razões para a adoção do RGPD[100].

A entrada em vigor do RGPD, em maio de 2016, não levou a uma alteração significativa dos recursos da CNPD (Gráfico I).

---

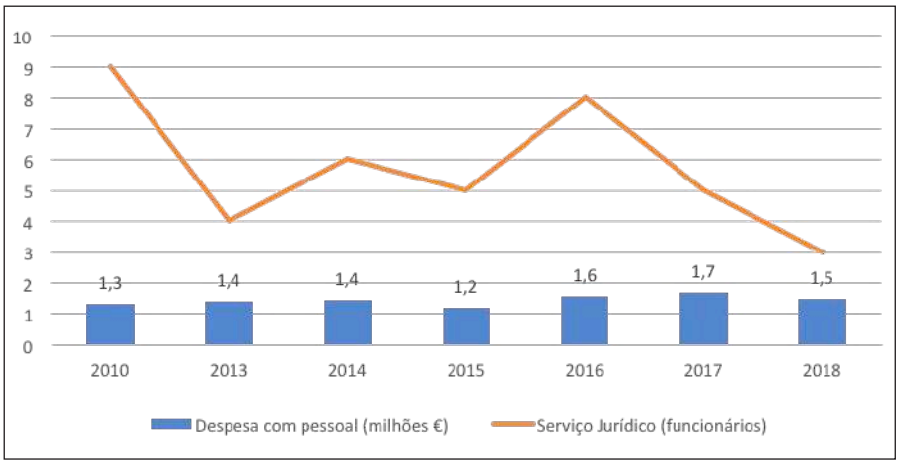
[97] Comunicação da Comissão ao Parlamento Europeu e ao Conselho, *Maior proteção, novas oportunidades – Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018*, de 24 de janeiro de 2018, COM(2018) 43 final, p. 12.

[98] Fundamental Rights Agency, *Data Protection in the European Union: the role of National Data Protection Authorities,* European Union Agency for Fundamental Rights, 2010, p. 42.

[99] Comissão Europeia, *Proteção da privacidade num mundo interligado. Um quadro europeu de proteção de dados para o século XXI,* COM(2012) 9 final, de 25 de janeiro de 2012, p. 8 ("Os recursos e as competências das autoridades nacionais de proteção de dados variam consideravelmente entre os Estados-Membros").

[100] Comissão Europeia, *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados)*, COM(2012) 11 final, de 25 de janeiro de 2012, p. 5 ["Segundo a avaliação de impacto, a execução (de um novo regulamento) deve conduzir, *inter alia*, a melhorias consideráveis quanto (...) à eficácia do controlo e da aplicação das regras em matéria de proteção de dados"].

Gráfico I
Evolução dos recursos humanos e financeiros da CNPD



Fonte: relatórios de atividades da CNPD, disponíveis em www.cnpd.pt.

O volume de despesa com pessoal da CNPD tem-se mantido estável desde 2010. Particularmente significativa vem a ser a redução para um terço do número de juristas, uma vez que estes são, a par dos técnicos de informática, os recursos humanos mais relevantes das autoridades de controlo[101]. Três juristas e quatro informáticos – num universo de 20 trabalhadores[102] – não são suficientes para responder às obrigações de supervisão que o RGPD impõe, justificando a afirmação da presidente da CNPD de que com estes recursos a autoridade de controlo portuguesa não

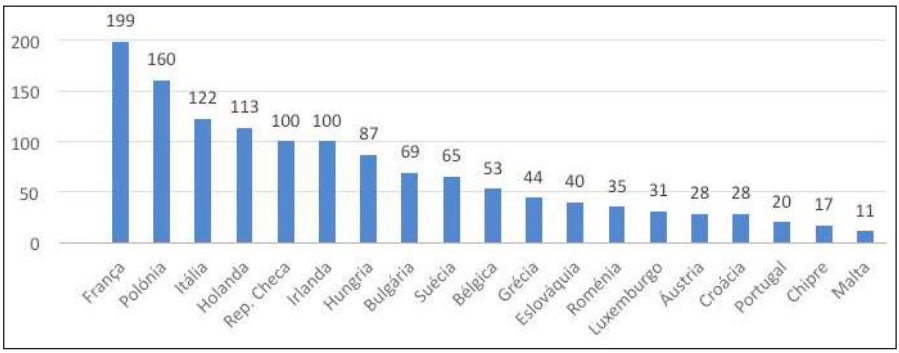
[101] Uma proposta de alteração do Parlamento Europeu previa a inclusão no considerando 120 RGPD da obrigação dos Estados-Membros garantirem, em particular, "as competências técnicas e jurídicas" das autoridades de controlo (Parlamento Europeu, *Relatório sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral de proteção de dados)*, de 21 de novembro de 2013, COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), p. 47).

[102] Comissão Nacional de Proteção de Dados, *Relatório de Atividades 2017/2018*, cit., p. 34.

tem condições "para fazer o que quer que seja no âmbito do regulamento que seja verdadeiramente uma tutela eficaz dos direitos fundamentais"[103].

A exiguidade dos recursos humanos da CNPD é manifesta quando observada em termos comparados (Gráfico II).

Gráfico II
Funcionários (2018)



Fonte: EUobserver[104].

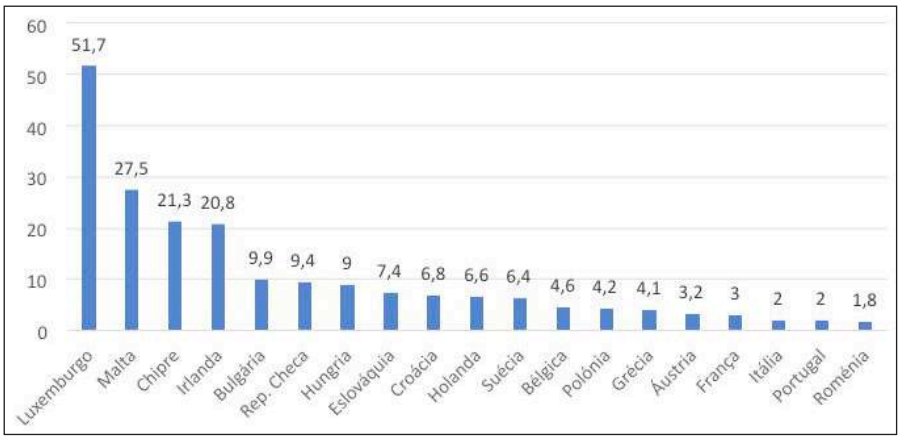
Em número de funcionários, a autoridade de controlo portuguesa é uma das mais pequenas da União Europeia, sendo dez vezes mais pequena do que a francesa, cinco vezes mais pequena do que a holandesa e duas vezes mais pequena do que a eslovaca. Uma das explicações para a reduzida dimensão dos recursos humanos da CNPD pode estar correlacionada com a dimensão populacional de Portugal, pelo que se introduziu esta variável com o intuito de calcular o seu valor relativo. Os resultados são esclarecedores (Gráfico III).

---

[103] Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, "Audição de Filipa Calvão (...)", 18 de maio de 2018, cit., 23:19 a 23:25.

[104] NIELSEN, Nikolaj e TEFFER, Peter, "Are EU data watchdogs staffed for GDPR", *EUobserver*, de 22 de maio de 2018. Não foram considerados os dados relativos à autoridade de controlo do Reino Unido (528,5 funcionários), uma vez que se trata de um Estado que entretanto abandonou a União Europeia, e os dados relativos à Alemanha (160,5 funcionários em 2017), Letónia (25 funcionários em 2017) e Dinamarca (35 funcionários em 2015), por não serem relativos a 2018.

Gráfico III
Funcionários por milhão de habitantes (2018)



Fonte: EUobserver (funcionários)[105]; Eurostat (população)[106].

Uma vez que as exigências decorrentes da aplicação do RGPD são idênticas em todos os Estados-Membros, com a introdução do elemento de escala população seria lógico pressupor que Estados com menor população tivessem proporcionalmente um número mais elevado de funcionários nas respetivas autoridades de controlo. Com efeito, uma autoridade de controlo tem de empregar um número mínimo de funcionários para exercer eficazmente as atribuições que lhe são conferidas pelo RGPD. Por esta razão, seria expectável que os Estados-Membros da União com menos de um milhão de habitantes – Luxemburgo, Malta e Chipre – fossem também aqueles que apresentam um número relativo mais elevado de funcionários.

O Gráfico III revela que a autoridade de controlo portuguesa tem um número relativo de funcionários apenas semelhante às autoridades italiana e romena, que corresponde a um décimo da irlandesa e a um

[105] Ibidem.

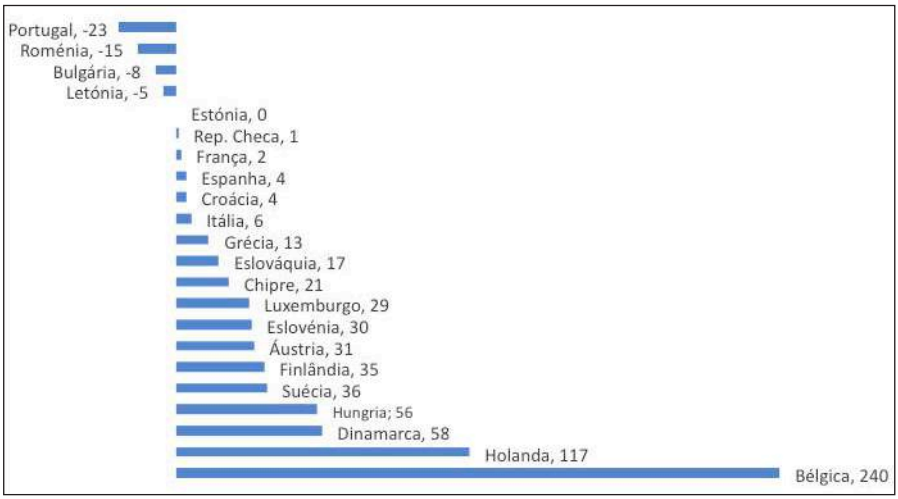
[106] Eurostat, *Population on 1 January*.

quinto da búlgara, dois Estados-Membros que têm, respetivamente, dos custos laborais mais elevados e mais baixos da União[107].

A análise comparada da evolução dos recursos humanos entre o período da entrada em vigor e da aplicação do RGPD (2016-2018) revela, por outro lado, que os problemas de funcionamento da CNPD se têm vindo a agravar (Gráfico IV).

Gráfico IV

Evolução % dos recursos humanos das autoridades de controlo (2016-2018)



Fonte: Deloitte[108].

A maioria dos Estados-Membros antecipou o início de aplicação do RGPD reforçando, em alguns casos exponencialmente (Bélgica e Holanda), os recursos humanos das suas autoridades de controlo. Apenas quatro Estados-Membros estiveram em contraciclo, incluindo Portugal, que foi o Estado-Membro que, inexplicavelmente, mais desinvestiu no

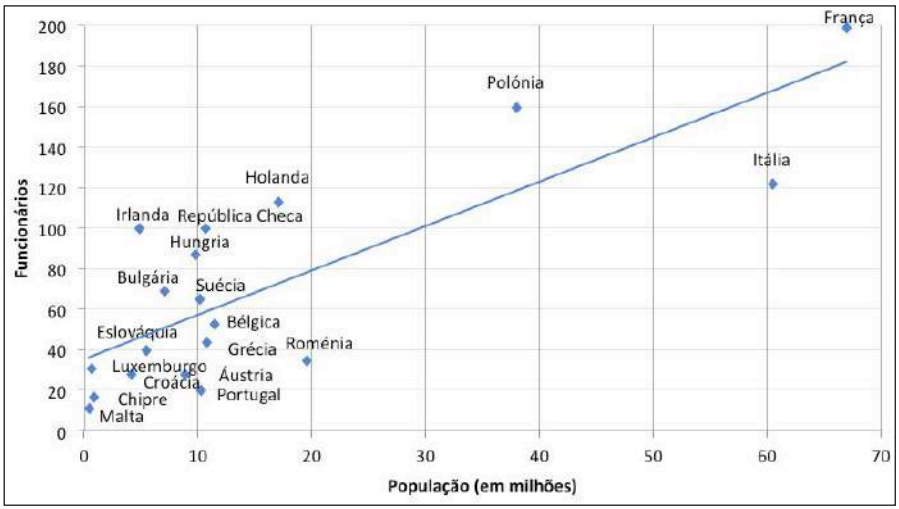
[107] O custo horário estimado do trabalho no setor privado em 2018 foi de 5,4€ na Bulgária, 14,2€ em Portugal e 32,1€ na Irlanda (Eurostat, *Hourly labor costs, 2018*).

[108] Deloitte, *Report on EU Data Protection Authorities. Part 4. Resources*, p. 6.

fortalecimento dos recursos humanos da sua autoridade de controlo no período crítico de adaptação a um novo quadro regulatório[109].

Por último, a linha de regressão do Gráfico V, para além de demonstrar a existência de uma correlação estatística forte entre as variáveis população e número de funcionários das autoridades de controlo, apresenta a CNPD com um resultado estatístico anormal (*outlier*). Para se situar na média das autoridades de controlo de Estados-Membros com a dimensão populacional de Portugal, a CNPD teria de triplicar os seus recursos humanos.

Gráfico V
População e funcionários (2018)



Fonte: EUobserver (funcionários)[110]; Eurostat (população)[111].

---

[109] Neste sentido, a opinião de Luís Neto Galvão em entrevista a Frederico Pedreira, *Advocatus*, de 13 de dezembro de 2019, p. 35, "(...) o RGPD foi aprovado em 2016 e já antes de 2016 já era conhecido por todos que íamos ter uma alteração substancial do paradigma. (...) Portugal era conhecedor disso, até porque a proposta da Comissão Europeia era de 2012, tivemos um logo caminho de adoção e de 2016 para cá sabíamos que tínhamos de adotar um conjunto de medidas. Desde logo capacitar a CNPD para lhe permitir ser um veículo de difusão, divulgação, esclarecimento de questões relacionadas com o RGPD e nada se fez".

[110] Nikolaj Nielsen e Peter Teffer, "Are EU data watchdogs staffed for GDPR", cit.

[111] Eurostat, *Population on 1 January*.

III. As alterações introduzidas pela lei de execução na lei de organização e funcionamento da CNPD são um passo decisivo para a criação de condições para o funcionamento efetivo da autoridade de controlo portuguesa. A CNPD foi investida de autonomia financeira e administrativa (art. 2.º, n.º 1, da Lei n.º 43/2004), garantia estrutural de independência, que vai finalmente permitir-lhe desenvolver o essencial da sua atividade sem depender de decisões administrativas de autorização de despesa oriundas de entidades que fiscaliza (e sanciona). Por outro lado, a orgânica da CNPD está agora adaptada ao modelo de supervisão criado pelo RGPD[112], destacando-se o surgimento dos departamentos de direitos e sanções, de inspeção e de relações públicas e internacionais (art. 22.º, n.º 1, als. a) a c) da Lei n.º 43/2004).

Permanecem, contudo, constrangimentos à contratação de pessoal qualificado relacionados com a escassez de funcionários públicos com "elevada competência profissional e experiência válida para o exercício da função" que possam ser recrutados em comissão de serviço, requisição ou destacamento (art. 30.º, n.ºs 2 e 3, da lei de execução). A qualidade do recrutamento externo pode também sair prejudicada pela pouca competitividade face ao setor privado das remunerações que podem ser pagas a consultores[113]. O reforço de recursos humanos estará, por último, fortemente condicionado enquanto se mantiverem as limitações à contratação de trabalhadores previstas em norma de execução orçamental (*v. g.* art. 157.º do Decreto-Lei n.º 84/2019, de 28 de junho).

Os problemas de funcionamento da CNPD vão também persistir se o seu orçamento não aumentar substancialmente. A drástica perda de receita própria, que passou de 2.668.155€ (2017) para 75.000€ (2019) em resultado da extinção da taxa de notificação de tratamentos, foi compensada por um aumento das transferências diretas do orçamento da Assembleia da República, que em 2019 compunham cerca de 93% das receitas da CNPD[114]. O início de aplicação do RGPD e a entrada em

---

[112] Filipa Calvão, "O RGPD e o Papel da Comissão Nacional de Proteção de Dados", *Revista de Direito Administrativo*, 4, janeiro-julho de 2019, pp. 68-70.

[113] Aproximadamente €2.600/mês, nos termos dos arts. 31.º, n.º 1, 32.º, n.º 1, e do mapa I anexo à lei de execução.

[114] Comissão Nacional de Proteção de Dados, *Plano de Atividades 2019*, 30 de outubro de 2018.

vigor da lei de execução não levou, no entanto, a qualquer incremento significativo do nível de despesa da autoridade de controlo portuguesa: para o ano de 2019, a CNDP previa um aumento da despesa de 15% (aproximadamente 300.000€) em relação a 2017[115]. Ainda que o RGPD tenha aumentado substancialmente o montante das coimas aplicáveis, as quais revertem em 40% para a CNPD (art. 42.º da lei de execução), a capacidade inspetiva da CNPD – e o consequente aumento de receitas que naturalmente daí decorra – está dependente de um reforço de meios humanos que só pode ocorrer através do aumento das transferências orçamentais que recebe da Assembleia da República.

Mas qual deve ser então o orçamento da CNPD? Na ausência de indicadores que possam ser utilizados para mensurar o nível de adequação dos recursos das autoridades de controlo nacionais, o Grupo de Trabalho do Artigo 29.º sugeriu um método de cálculo dos respetivos orçamentos, que deve resultar da soma de um montante fixo que cubra funções básicas de funcionamento, e um montante variável baseado numa fórmula relacionada com a população dos Estados-Membros, o PIB e o número de multinacionais estabelecidas no respetivo território[116].

Considerações finais

A Comissão Europeia tem repetidamente declarado que não hesitará em utilizar todos os instrumentos que tem à sua disposição, incluindo ações por incumprimento, para garantir que as reformas legislativas adotadas pelos Estados-Membros no âmbito do direito da proteção de dados estão em conformidade com o direito da União e não se transformam num exercício de "sobrerregulamentação" (*gold-plating*)[117].

---

[115] Comissão Nacional de Proteção de Dados, *Relatório de Atividades 2017/2018*, cit., p. 36 e *Plano de Atividades 2019*, cit., p. 18.

[116] Grupo de Trabalho do Artigo 29, *Opinion 1/2012 on the Data Protection Reform Proposals*, de 23 de março de 2013, WP 191, p. 17.

[117] Comunicado de Imprensa da Comissão Europeia, "General Data Protection Regulation shows results, but work needs to continue", de 24 de julho de 2019. A Comissão identifica o gold-plating com os custos desnecessários para as empresas e as entidades públicas causados pela ultrapassagem pelos Estados-Membros do "estritamente requerido pela legislação da (União), quando a transpõem para a ordem jurídica interna" [Comunicação da Comissão ao

Em janeiro de 2018, advertiu que iria especificamente fiscalizar se os Estados-Membros "tomam as medidas necessárias previstas nos termos do (RGPD), se (se) atrasam a tomar essas medidas ou (se) recorrem às cláusulas de especificação previstas nos termos do regulamento de forma contrária ao regulamento"[118]. O silêncio da Comissão perante o manifesto preenchimento pelo Estado português de todas estas condições durante o conturbado – a adjetivação não me parece excessiva – processo de implementação do RGPD é, por isso, ensurdecedor.

A inércia da Comissão apresenta-se particularmente problemática porque a missão de assegurar a aplicação uniforme do RGPD e a tutela dos direitos que reconhece aos titulares de dados pessoais está, em primeira linha, entregue em Portugal a uma autoridade administrativa independente que tem problemas crónicos de funcionamento relacionados com a escassez dos seus recursos humanos.

A "guardiã do direito à proteção de dados" na ordem jurídica portuguesa está seguramente limitada, mas não completamente manietada, como o demonstra a decisão de desaplicação de parte da lei de execução do RGPD em cumprimento do mandato "*Costanzo*" ou a influência que teve no veto presidencial às alterações introduzidas no regime jurídico aplicável ao tratamento de dados pelo sistema judicial[119]. Mas a fiscali-

---

Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, *Legislar melhor para obter melhores resultados – agenda da UE*, de 19 de maio de 2015, COM(2015) 215 final, p. 8].

[118] Comunicação da Comissão ao Parlamento Europeu e ao Conselho, *Maior proteção, novas oportunidades – Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018*, cit., p. 10. A Comissão tem estado particularmente atenta à implementação da Diretiva (UE) 2016/680, de 27 de abril, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, tendo inclusivamente iniciado ações por incumprimento contra a Espanha (C-658/19) e a Grécia por atraso na transposição da diretiva. Portugal transpôs a Diretiva 2016/680 (mais de um ano fora de prazo) através da Lei n.º 59/2019, de 8 de agosto.

[119] Casa Civil do Presidente da República, Ofício n.º 9353, de 26 de julho de 2019. O Presidente da República considerou que a exclusão do Ministério Público do controlo da CNPD é desconforme ao RGPD, argumento invocado pela CNPD no Parecer n.º 25/2018, de 28 de maio, sobre a Proposta de Lei 126/XIII/3.ª(GOV), que "altera o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial".

zação efetiva do cumprimento do RGPD não passará de uma quimera enquanto a Assembleia da República não reforçar substancialmente as dotações orçamentais anuais que transfere para a CNPD. No atual contexto de conflito institucional entre a CNPD e o parlamento, tal reforço provavelmente só surgirá por via de um impulso externo que só a "guardiã dos Tratados" pode vir a dar.

A anonimização enquanto mecanismo de proteção de dados pessoais à luz da atual conjuntura legislativa europeia

Augusto Cesar Torbay*

Resumo: Consubstanciando uma exceção ao âmbito de aplicação material do RGPD, os dados anonimizados expressam uma solução de compromisso entre a tutela das pessoas singulares e a maleabilidade dos dados pessoais. Contudo, este Regulamento acaba por afastar-se de uma noção absoluta de anonimização, deixando-a aberta a uma ponderação de razoabilidade de meios. Partindo desta premissa, e observando que a concretização desse critério tem uma expressão direta no nível de proteção prestada aos respetivos titulares, procuraremos revisitar a questão da anonimização de dados pessoais no sentido de aferir da valência atual do respetivo regime, sem perder de vista os recentes contributos científicos que denunciam a sua incontornável fragilidade.

Palavras-chave: *Dados pessoais, Dados anonimizados, Anonimização de dados, Identificabilidade, RGPD.*

Abstract: Established as an exception to the material scope of the GDPR, anonymized data expresses a compromise between the protection of data subjects and the malleability of personal data. However, this Regulation departs from an absolute conception of anonymization, leaving it open to an assessment regarding the reasonable means likely

* Encarregado de Proteção de Dados junto da Autoridade Nacional de Segurança Rodoviária. Licenciado em Direito, Pós-graduado em Direito Comercial e Mestre em Direito Forense pela Faculdade de Direito da Universidade Católica Portuguesa de Lisboa, encontrando-se presentemente a frequentar o curso de Doutoramento na mesma instituição. Frequentou a 3.ª edição do Curso Breve sobre Proteção de Dados Pessoais organizado pela Associação da Faculdade de Direito da Universidade Nova de Lisboa (Jurisnova), bem como o curso de certificação de encarregados de proteção de dados promovido pelo European Centre on Privacy and Cybersecurity da Universidade de Maastricht. Iniciou a sua produção científica no campo da arbitragem internacional, encontrando-se, presentemente, a investigar e atuar na área da Tecnologia de Informação, Privacidade e Proteção de dados.

to be used to identify a natural person. Based on this premise, and observing that the execution of this criterion has a direct implication in the level of protection granted to data subjects, we intend to revisit the issue of anonymization of personal data in order to assess the current validity of the respective regime, without losing sight of the recent scientific contributions that denounce its unavoidable fragility.

***Keywords**: Personal data, Anonymized data, Data anonymization, Identifiability, GDPR.*

Considerações iniciais

Um dos principais traços característicos da ciência do Direito é a natureza dialética dos impulsos que promovem o seu desenvolvimento. Como que estabelecendo um diálogo com a realidade efetiva que procura regular, o Direito desenvolve-se no intento de acompanhar a complexidade dinâmica da interação do ser humano em comunidade. Fadada ao contínuo desfasamento e desatualização, esta correlação catalisa o progresso do Direito e promove o desenvolvimento de soluções justas. No entanto, e muito embora a evolução das interações humanas tenham seguido um ritmo que permitiu ao Direito ir acompanhando o compasso das realidades que visava conformar, o advento de um contexto social de cariz eminentemente tecnológico e de pendor tendencialmente global, parece antever que o concreto teor destas relações observará uma transmutação tal que dificilmente poderá ser objeto do mesmo nível de acompanhamento legal do que outrora se verificava.

Uma vez transposta para o contexto das operações enquadradas no universo digital, a tarefa da racionalização do pensamento jurídico vê-se impreterivelmente complexificada pelo carácter dinâmico e volátil das relações jurídicas que se formam no seu seio. O desenvolvimento contínuo de novos recursos e mecanismos de interação determina um panorama caótico, colocando o "legislador no intento constante de acompanhar o passo do desenvolvimento tecnológico"[1] na sua demanda por soluções

[1] BUTTARELLI, Giovanni. "Speech on "All we need is L....Privacy by design and by default", *Conferência RightsCon*, 2017, p. 4, disponível em: https://edps.europa.eu/data-protection/our-work/our-work-by-type/speeches-articles_en, acedido a: 27.02.2019.

que não sejam meramente justas, mas também flexíveis e ambivalentes, para assim lograr assegurar uma proteção eficaz do indivíduo.

Do nosso ponto de vista, encontramos uma expressão concreta desta dinâmica no enquadramento legal concedido pela legislação europeia ao regime da anonimização de dados pessoais. Transcorrido mais de um ano de aplicabilidade do RGPD[2], podemos afirmar que já se encontra enraizado na nossa consciência coletiva que, com este Regulamento, a UE procurou encetar um verdadeiro esforço de *empowerment* do titular dos dados.

Não deixa de ser igualmente evidente, porém, que o legislador europeu manteve presente que a proteção de dados não se subsume, como tal, a um valor absoluto, e que a realidade do presente enquadramento jurídico clama por um equilíbrio entre a proteção dos direitos fundamentais dos cidadãos e a promoção da liberdade dos atores comerciais que operam e promovem o ecossistema digital. Como que expressando uma solução de compromisso, e no sentido de permitir uma melhor maleabilidade de informações, o RGPD vem consagrar um regime de excecionalidade aos dados anonimizados, coartando-os da sua tutela e mantendo-os aquém dos direitos e obrigações que reconhece ao tratamento de dados pessoais.

Conforme procuraremos demonstrar no presente estudo, consideramos que é precisamente aqui que reside o desencontro entre o progresso legislativo e o substrato tecnológico que, em última análise, ameaça a coerência da tutela europeia consagrada à proteção de dados pessoais. O carácter excecional concedido às informações produzidas por um processo de anonimização decorre do prejuízo da identificabilidade destes dados, porém, somos crescentemente encarados com o facto de que as novas tendências computacionais[3], bem como a crescente disponibilização de dados públicos, contribuem para que a produção de dados eficientemente anonimizados se revista de uma crescente complexidade.

---

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

[3] OHM, Paul. "Broken promises of privacy: Responding to the surprising failure of anonymization", *UCLA Law Review*, v. 57, 2010, p. 1701-1777, disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006, acedido a: 21.02.2017.

Muito embora, a nível conceptual, o processo de anonimização pudesse consubstanciar o perfeito equilíbrio entre a proteção do titular dos dados e a maleabilidade da informação, ao arrepio da confiança que o legislador europeu lhe reconheceu, torna-se cada vez mais evidente que existe uma crescente unicidade de vozes que se levanta relativamente ao declínio da valência da anonimização de dados pessoais e que denuncia uma tendência para a efetiva impossibilidade de produção de dados que, além de anónimos, logrem suster utilidade.

Nesta medida, pretendemos dedicar o presente estudo à observação do regime dos dados pessoais anonimizados, procurando ponderar a valência da conceptualização do processo de anonimização, bem como a sua efetividade na tutela dos direitos dos titulares dos dados. Aproveitaremos também o presente ensejo para, à luz dos contributos científicos evidenciados ao longo dos últimos anos, aferir se poderia ser efetivamente pertinente uma reponderação a nível da abordagem europeia em relação a esta matéria[4].

1. O regime jurídico dos dados pessoais anonimizados no âmbito do RGPD

A base fundamental da aplicação material da tutela europeia relativa à proteção de dados pessoais (a qual é determinada pela conjunção do disposto no n.º 1 do art.º 2 com a noção estatuída pelo n.º 1 do art.º 4 do RGPD), subsume-se ao simples facto de que as disposições do Regulamento apenas serão aplicáveis ao tratamento de informações "relativa[s] a uma pessoa singular identificada ou identificável", entendendo-se, esta última, como uma "pessoa singular que possa ser identificada, direta ou indiretamente".

A consequência lógica que importa retirar desta abordagem é que, se uma determinada informação não concernir a uma pessoa singular

---

[4] ZIBUSCHKA, Jan; KUROWSKI, Sebastian; ROßNAGEL, Heiko; SCHUNCK, Christian H; ZIMMERMANN, Christian. "Anonymization Is Dead – Long Live Privacy" in ROßNAGEL, Heiko (Ed.); WAGNER, Sven (Ed.); HÜHNLEIN, Detlef (Ed.). *Gesellschaft für Informatik*, 2019, p. 71-82, disponível em: https://dl.gi.de/bitstream/handle/20.500.12116/20995/proceedings-06.pdf, acedido a: 23.07.2019.

identificada ou identificável, esta informação deverá ser considerada anónima e, como tal, não será compreendida no escopo material do RGPD. Contudo, não são apenas as informações anónimas que cabem neste regime. Nos termos avançados pelo considerando 26 deste Regulamento, considerar-se-ão igualmente desenquadradas do seu regime todos os dados que, embora possam ter sido considerados como pessoais, tenham sido "tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado". Na prática, isto se traduz no facto de que tanto os dados anónimos, como os anonimizados (ou seja, dados pessoais que foram submetidos a um processo de anonimização), não caberão no âmbito de aplicação material do RGPD.

Numa primeira análise, em termos estritamente conceptuais, esta determinação aparenta assentar as bases do processo de anonimização numa presunção de impossibilidade absoluta de reidentificação (consubstanciando um conceito de *guaranteed anonymisation*, conforme concetualizado pela doutrina[5]). Tal como sugere o parecer do Grupo de Trabalho sobre técnicas de anonimização[6], muito embora não exista uma norma prescritiva na legislação europeia que estatua a forma como este processo deve ser realizado, na sua abordagem encontra-se subjacente uma determinada notação de irreversibilidade[7].

Aliás, do nosso ponto de vista, e através de um exercício de interpretação sistemática, entendemos que o regime jurídico que é consagrado no quadro da legislação europeia de proteção de dados permite supor a propensão do legislador para uma conceção de anonimização "tão permanente quanto a eliminação"[8]. Nomeadamente, no âmbito do RGPD, esta correlação encontra expressão na própria consagração do princípio da limitação da conservação dos dados pessoais (*cfr.* alínea e) do n.º 1

---

[5] OHM, Paul. *op. cit.*, p. 7.

[6] Grupo de Trabalho, Parecer 05/2014 sobre técnicas de anonimização, 0829/14/PT, 10/03/2014, p. 7, disponível em: https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf, acedido a: 06.02.2019.

[7] Em certos domínios, a relação entre o processo de anonimização de dados pessoais e a exigência de irreversibilidade é expressa literalmente, como seja, nomeadamente, o caso da norma 29100:2011, que vem determinar que as informações sobre "pessoas identificáveis" devem ser "alteradas irreversivelmente" de modo a que as mesmas "já não possa[m] ser identificada direta ou indiretamente".

[8] Grupo de Trabalho, *op. cit.*, p. 6.

do art. 5.º). Ao contrário do que poderia ser empiricamente expectável, esta norma não determina a obrigatoriedade de eliminação dos dados pessoais após o "período necessário para as finalidades para as quais são tratados". O que efetivamente se estatui é a proibição da sua conservação numa "forma que permita a identificação dos titulares dos dados". Em concreto, o que se determina nesta disposição é que, de acordo com o princípio da limitação da conservação dos dados pessoais, após o termo do referido período, o responsável pelo tratamento deverá proceder ao apagamento dos dados ou, em alternativa, promover a sua anonimização. Salvo melhor entendimento, ao estatuir a anonimização como alternativa à eliminação, o legislador europeu demostra a expectativa de um processo de anonimização tão eficiente quanto a eliminação dos dados.

Mutatis mutandis, observamos esta mesma equiparação no regime consagrado ao tratamento de dados de tráfego no sector das comunicações eletrónicas. Conforme o n.º 1 do art.º 6 da Diretiva 2002/58/CE[9], estes dados "devem ser eliminados ou tornados anónimos" quando deixem de ser necessários para efeitos da transmissão da comunicação aos quais se referem. Por sinal, e nos termos da Proposta de Regulamento referente a esta matéria e que se prevê que venha a revogar a referida Diretiva 2002/58/CE[10], este mesmo entendimento será consagrado, não apenas quanto aos dados referentes ao conteúdo das comunicações eletrónicas, como também em relação aos respetivos metadados[11]. Por outro lado, importa salientar que a equiparação da anonimização à eliminação não é apenas transversal ao direito da União, verificando-se ainda a sua influência para lá das fronteiras da Europa. Nomeadamente, uma postura semelhante encontra-se vertida nos termos da alínea e) do n.º 4 do art.º 5.º da Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal do Conselho da Europa.

---

[9] Diretiva n.º 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.

[10] 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.

[11] *Cfr.* n.º 1 e 2 do art. 7.º da Proposta de Regulamento.

Com base nestas evidências, entendemos que seria possível supor que o carácter de irreversibilidade se encontraria no âmago da noção europeia de anonimização, como *conditio sine qua non* da sua efetividade[12]. Não obstante, através dos contributos dos respetivos considerandos, o RGPD vem afastar-se desta noção estrita de anonimização[13]. Procurando favorecer uma conceção mais maleável, o legislador europeu estatui uma solução de compromisso através de uma conceptualização fundamentada numa ponderação de razoabilidade e cujos vetores se encontram delimitados pelo próprio conceito de identificabilidade[14].

No contexto do mencionado considerando 26, o Regulamento vem determinar que, para que um dado possa ser considerado anonimizado, não será necessário que o respetivo titular "não seja ou já não possa ser identificado" em termos absolutos. Em concreto, para efeitos desta abordagem, bastará que, observando "todos os meios suscetíveis de ser razoavelmente utilizados (...) quer pelo responsável pelo tratamento quer por outra pessoa" o respetivo titular dos dados não possa ser direta ou indiretamente identificado. Ou seja, e conforme referido acima, a chave da ponderação centra-se na avaliação do que é "razoável" de ser utilizado para efeitos da identificação. O que verdadeiramente ocorre perante esta consagração é uma flexibilização do conceito, o qual, necessariamente, fica na dependência de um juízo de ponderação dos recursos disponíveis para a reversão do processo.

Enquanto direito fundamental, o direito à proteção de dados pessoais não é, em si, absoluto. Estando aberto à ponderação de juízos de

---

[12] Grupo de Trabalho, *op. cit.*, p. 7.

[13] Tal como refere o Advogado-Geral Maciej Szpunar nas conclusões apresentadas em 21 de março de 2019 no âmbito do processo C-673/17 do TJUE, muito embora, na ordem jurídica da União, os considerandos se encontrem desprovidos de natureza prescritiva e, como tal, não possuam valor jurídico independente, a verdade é que representam uma ferramenta obrigatória na interpretação das disposições de um ato jurídico da união (Conclusões do Advogado-Geral Maciej Szpunar de 21 de março de 2019, *Planet49 GmbH contra Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* C-673/17, ECLI:EU:C:2019:246, para. 71).

[14] PURTOVA, Nadezhda. "The law of everything. Broad concept of personal data and future of EU data protection law". *Law, Innovation and Technology*. v. 10, n.º 1, 2018, p. 40-81, disponível em: https://doi.org/10.1080/17579961.2018.1452176, acedido a: 17.03.2019.

proporcionalidade[15], compreende-se a intenção do legislador europeu em favorecer uma relação de compromisso entre a tutela deste direito e os interesses na maleabilidade dos dados. Contudo, a abertura deste conceito a uma lógica assente num critério de razoabilidade torna evidente que uma dimensão de risco será sempre uma realidade inerente ao próprio processo de anonimização[16], pelo que, permitimo-nos suspeitar que esta sujeição à indeterminação poderá representar uma fragilidade que não se coadune com o regime de excecionalidade que é consagrado aos dados anonimizados à luz do RGPD.

Esbatendo a fronteira que demarca a anonimização da pseudonimização[17] (a qual, no seu cerne, se caracteriza pela possibilidade de reidentificação através de um atributo único) cria-se um *tertium genus* localizado entre ambos os conceitos e que, no fundo, se carateriza pela nomenclatura do primeiro e pelo risco inerente do segundo.

No essencial da sua conceptualização, deveria ser esta dimensão de risco que demarcaria a anonimização da pseudonimização. Ao reduzir a possibilidade de "ligação entre um conjunto de dados e a identidade original de um titular", esta última, representa uma "medida de segurança útil, porém, não consubstancia um método de anonimização de dados pessoais"[18]. Conforme evidenciado pelas investigações realizadas em torno do já clássico caso de publicação de registos da Comissão de Táxis e Limusines de Nova Iorque em 2014[19], o recurso à pseudonimização

---

[15] HANSSON, Mats; LOCHMULLER, Hanns; RIESS, Olaf; SCHAEFER, Franz; ORTH, Michael; RUBINSTEIN, Yaffa; MOLSTER, Caron; DAWKINS, Hugh; TARUSCIO, Domenica; POSADA, Manuel; WOODS, Simon. "The risk of re-identification versus the need to identify individuals in rare disease research", *European Journal of Human Genetics.* 24, 2016, p. 1553-1558, disponível em: https://www.ncbi.nlm.nih.gov/pubmed/27222291, acedido a: 17.03.2019.

[16] Grupo de Trabalho, *op. cit.*, p. 7.

[17] A qual, nos termos do n.º 5 do art. 4.º do RGPD, se concretiza no tratamento de dados tendente a impossibilitar a sua atribuição a um titular de dados específico sem o auxilio de informações suplementares, as quais, deverão ser mantidas separadamente e sujeitas a medidas técnicas e organizativas que assegurem a permanência da pseudonimização dos dados.

[18] Grupo de Trabalho, *op. cit.*, p. 22.

[19] Em 2014 a comissão de táxis e limusines de Nova Iorque publicou uma base de dados com registos relativos a todas as viagens realizadas nessa cidade durante um ano. Com intuito de promover a proteção dos titulares dos dados envolvidos, procurou-se realizar a pseudonimização através da utilização de uma função criptográfica *hash* sobre determinados elementos, em particular, o número identificativo da viatura e o número da licença do respetivo

detém riscos próprios decorrentes da efetiva possibilidade de reidentificação[20]. Em consequência deste facto, e por consciência deste risco, o regime jurídico dos dados pseudonimizados não os afasta plenamente da tutela do RGPG.

Na nossa perspetiva, e avançando considerações que procuraremos explorar *infra*, consagrar um conceito de anonimização que se caracteriza, necessariamente, por uma dimensão omnipresente de risco poderá revelar-se particularmente problemática, principalmente se mantivermos presente que os dados anonimizados contornam a tutela consagrada pelo RGPD. Muito embora este Regulamento declare a sua intenção de prestar uma tutela real e efetiva aos titulares dos dados, consideramos que a consagração de uma noção frágil de anonimização poderá concorrer para o desenvolvimento de um ambiente de insegurança jurídica, como resultado da possível frustração das expectativas depositadas na viabilidade das garantias prestadas pelo processo de anonimização.

2. A viabilidade efetiva da conceção europeia de anonimização de dados pessoais

Assente na ideia de impossibilidade prática de alcançar dados absolutamente anonimizados, e procurando obviar um regime demasiado estrito, o legislador europeu concebeu uma solução fundamentada num entendimento relativo de anonimização. Caberá, no entanto, questionar se esta abordagem é efetivamente operacional ou se, pelo contrário, a

---

condutor. Como a função *hash* representa uma relação de muitos para um, a complexidade na sua reversão encontra-se na dimensão do universo de pesquisa na qual se enquadra. Quando o *input* da função é considerável, a reversão vê-se complexificada e, consequentemente, são promovidas as garantias de segurança. Neste caso, porém, o universo em questão, ou seja, o número de condutores de táxis, embora empiricamente substancial, não representou obstáculo definitivo à descoberta do algoritmo de pseudonimização, tendo-se logrado a reversão com o recurso a informações publicamente disponíveis.

[20] NALDI, Maurizio. "Anonymization Systems and Utility", conferência IPEN de 12 de junho de 2019, sobre o tema *"State of the art" in data protection by design – Current state and future trends*, Itália. Apresentação disponível em: https://edps.europa.eu/sites/edp/files/publication/12-06-19_maurizio-naldi_anonymization-systems-and-utility_en.pdf, acedida a: 27.07.2019.

indeterminação do critério ao qual se submete se reveste de uma complexidade tal que, na prática, acabe por desembocar igualmente numa condição impossível de atingir.

No sentido de nos permitir tecer considerações concretas quanto à efetiva viabilidade da noção europeia de anonimização de dados, e assumindo como premissa o critério da razoabilidade de meios consagrado pelo RGPD, no presente ponto, procuraremos analisar – de forma necessariamente sumária – aqueles que se nos evidenciam como os principais obstáculos e dificuldades à produção de dados eficientemente anonimizados.

2.1. A inexistência de um padrão determinado para um processo de anonimização eficiente

Ao colocar as bases do processo de anonimização num critério de razoabilidade de meios, o legislador vem determinar que a anonimização deverá considerar-se alcançada apenas quando o panorama do contexto concreto do tratamento e as circunstâncias específicas que influem sobre a identificabilidade permitam considerar que a reidentificação se tornou "razoavelmente impossível"[21]. Contudo, além da conceptualização deste critério, parece-nos indiscutível que não dispomos de um padrão viável que nos permita antever qual o procedimento apropriado para lograr esse nível de anonimização. Da mesma forma, não existe uma predeterminação que indique quais os recursos considerados necessários para a reversão ou que permita a construção de um modelo concreto de aferição da robustez de uma determinada estratégia de anonimização[22].

A verdade, porém, é que a inexistência de tal roteiro não se encontra inteiramente desprovida de sentido. Se atendermos ao facto de que esta área é um campo em pleno desenvolvimento, cujas fronteiras se encontram em constante reformulação em decorrência da contínua investigação de que é alvo[23], facilmente se compreende que uma concretização de um modelo uniforme de anonimização não se revelaria como uma

---

[21] Grupo de Trabalho, *op. cit.*, p. 9.

[22] *Ibid.*, p. 30.

[23] PURTOVA, Nadezhda, *op. cit.*, p. 78.

efetiva mais-valia pois, rapidamente, observar-se-ia a sua condenação à desadequação prática e consequente ineficácia. Principalmente por se fundamentar numa ponderação de razoabilidade, o conceito de anonimização consagrado no âmbito do RGPD torna-se uma realidade dinâmica que encontra os seus fundamentos operacionais na capacidade informática de processamento de informação e que, como tal, exige uma ponderação flexível e contínua, que não se coaduna com uma medida uniforme e estática de anonimização.

No entanto, o carácter flexível desta abordagem tem como consequência necessária a indeterminação do conceito de anonimização que, em determinados casos, se apresenta como um elemento incontornável. É precisamente neste sentido que vão proliferando na doutrina[24] casos de estudo que evidenciam a extrema dificuldade de criar uma base de dados com um nível de anonimização satisfatório[25].

Ao entregar o conceito de anonimização de dados pessoais a uma ponderação de razoabilidade de meios de identificação, a legislação europeia vem determinar uma dimensão de complexidade ao procedimento que poderá, em última análise, ser intransponível. Nos termos desenvolvidos pelo referido considerando, a avaliação da razoabilidade da reversão do processo deverá ser realizada numa perspetiva eminentemente global, atenta à uma universalidade de elementos dinâmicos e voláteis, que deverá ser mantida ao longo do tempo. Perante uma tal exigência, a inexistência de vetores de orientação concretos poderá entregar esta ponderação a uma dimensão necessariamente subjetiva, de validade efémera e, nessa medida, propensa à incerteza e ao risco.

2.2. A universalidade de elementos que influem na avaliação do critério da razoabilidade de meios

Concretizando aquele que é um dos poucos vetores de orientação que o Regulamento nos presta nesta matéria, o seu considerando 26 procura

---

[24] ROCHER, Luc; HENDRICKX, Julien M.; MONTJOYE, Yves-Alexandre de. "Estimating the success of re-identifications in incomplete datasets using generative models". *Nature Communications.* v. 10, n.º 3069, 2019, p. 2, disponível em: https://www.nature.com/articles/s41467-019-10933-3, acedido a: 30.07.2019.

[25] Grupo de Trabalho, *op. cit.*, p. 3.

evidenciar que todo o processo de anonimização de dados pessoais estará pendente de uma avaliação eminentemente multidimensional. A premissa, como já sabemos, é a ponderação transversal que o responsável deverá encetar e que, necessariamente, terá de compreender a totalidade dos meios razoavelmente utilizáveis para efeitos de identificação direta ou indireta. Contudo, na sua concretização, esta avaliação não se poderá limitar à perspetiva do próprio responsável pelo tratamento, uma vez que deverão ser trazidos à colação os recursos identificativos de eventuais terceiros que possam ter acesso legal aos dados em causa.

Em termos concretos, o que se deve retirar desta construção é que o legislador comunitário procurou consagrar uma abordagem integral ao processo de anonimização, estatuindo como que um "dever de meios" (implementação dos meios considerados razoáveis para garantir a robustez da anonimização) mais do que de um "dever de resultados"[26] (produção de dados absolutamente anónimos). Através de um exercício de ponderação global, que não considere apenas elementos intrínsecos à informação em causa (como seja, nomeadamente, a própria natureza dos dados a tratar), mas igualmente fatores eminentemente extrínsecos (como o enquadramento contextual do tratamento), o legislador da União pretende que o responsável possa garantir que, embora não seja impossível, a identificação dos dados implicaria um esforço desrazoável.

Do nosso ponto de vista, a transversalidade exigida à ponderação dirige-nos à conclusão de que o sucesso da anonimização dependerá sempre da relação entre as particularidades dos próprios dados e os elementos contextuais que enquadram o tratamento[27]. Nesta linha de raciocínio, pretendemos dedicar o presente título à observação destes elementos, no sentido de aferir da sua influência no processo de anonimização.

---

[26] ELLIOT, Mark; MACKEY, Elaine; O'HARA, Kieron; TUDOR, Caroline. *The Anonymisation Decision-Making Framework*, University of Manchester, GB. UKAN, 2016, p. 18.

[27] *Ibid.*, p. 52.

2.2.1. A influência de elementos de carácter extrínseco: A consideração de fatores contextuais do processo de anonimização

Revestindo-se a anonimização de um cariz complexo e interrelacionado, torna-se evidente que uma avaliação de elementos contextuais (como sejam, nomeadamente, os agentes envolvidos, o tipo de procedimentos implementados ou as infraestruturas disponíveis) seja um elemento essencial à sua ponderação. Aliás, o carácter evolutivo e dinâmico da ciência da computação, bem como a sua capacidade de processamento de informação e, consequentemente, a complexificação dos dados objeto de tratamento, exigem que o respetivo responsável se retenha especialmente na avaliação do contexto tecnológico que compagina o conjunto dos meios suscetíveis de serem razoavelmente utilizados para efeitos de identificação. Como consequência direta desta relação, é hoje evidenciado pela doutrina que o desenvolvimento tecnológico enforma a noção de privacidade e confidencialidade[28]. Mais, em virtude da contínua investigação levada a cabo neste campo, assiste-se a um constante redefinir das fronteiras do que é razoavelmente expectável de ser realizado, observando-se uma continua potencialização de recursos, diminuição de custos e aumento de especialização[29].

Chegamos a encontrar opiniões que denunciam que, na maior parte das bases de dados confiadas como anonimizadas, a identificação não requer mais do que conhecimentos de estatística básica e programação[30]. Desta forma, facilmente se antevê a possibilidade de que determinadas avaliações (realizadas, naturalmente, no momento da anonimização), possam vir a ser postas em causa e, consequentemente, prejudicar a

---

[28] ZIMMERMANN, Christian; CABINAKOVA, Johana; "A Conceptualization of Accountability as a Privacy Principle" in ABRAMOWICZ W. (eds) *Business Information Systems Workshops. Lecture Notes in Business Information Processing*, v. 228, 2015, p. 261–272, disponível em: https://www.semanticscholar.org/paper/A-Conceptualization-of-Accountability-as-a-Privacy-Zimmermann-Cabinakova, acedido a: 22.08.2019.

[29] Grupo de Trabalho, *op. cit.*, p. 9.

[30] NARAYANAN, Arvind; FELTEN, Edward W. *No silver bullet: De-identification still doesn't work*, 2014, p. 6, disponível em: https://iapp.org/resources/article/no-silver-bullet-de-identification-still-doesnt-work, acedido a: 27.07.2018.

proteção dos respetivos titulares[31]. Apenas considerando o contexto tecnológico no qual se enquadra o tratamento é possível tentar alcançar uma relação eficiente entre os esforços necessários à anonimização de dados pessoais e os recursos exigidos para a sua reversão (como o custo, o saber-fazer ou o tempo)[32].

Uma falácia comum, que assenta na desconsideração do carácter evolutivo do enquadramento tecnológico, é julgar que a anonimização é um estado determinado em que um particular conjunto de dados se encontra[33]. Muito pelo contrário, a verdade é que o ritmo acentuado do desenvolvimento "da capacidade computacional e das ferramentas disponíveis"[34] demanda uma aproximação dinâmica a esta questão e, principalmente, o reconhecimento de que a anonimização possui uma propriedade eminentemente volátil, que não deve ser apenas atingida, como também mantida no tempo.

As considerações de cariz contextual, porém, não se devem limitar à avaliação do *status quo* dos recursos tecnológicos, mas também ao manancial de informação disponível que poderá influenciar a reidentificação da informação anonimizada. Tal como evidenciado por múltiplas investigações, encontra-se hoje perfeitamente demostrada a efetiva possibilidade de identificar informação anonimizada com recurso a bases de dados públicas[35].

Devemos manter presente que na avaliação da razoabilidade de meios disponíveis para a identificação não está apenas em causa uma abordagem relativa do conceito de identificabilidade. Como vimos, para efeitos de reidentificação direta ou indireta, a ponderação de razoabilidade não deverá ser realizada apenas da perspetiva do responsável pelo tratamento[36].

---

[31] PORTER, C. Christine. "De-identified data and third party data mining: The risk of reidentification of personal information", *WashingtonJournal of Law, Technology & Arts,* 5, 2008, p. 3, disponível em: http://www.lctjournal.washington.edu/Vol5/a03Porter.html, acedido a: 27.07.2019.

[32] Grupo de Trabalho, *op. cit.*, p. 10.

[33] ELLIOT, Mark. *et al*, *op. cit.*, p. 1.

[34] Grupo de Trabalho, *op. cit.*, p. 7.

[35] HANSSON, Mats. *et al*, *op. cit.*, p. 1554.

[36] *Cfr. o* considerando 26 do RGPD.

Aprofundando estas considerações, o TJUE[37] veio consagrar que o carácter de identificabilidade não dependerá apenas dos meios próprios de uma determinada pessoa, mas deverá ser observada também a suscetibilidade de identificação decorrente da combinação com outros recursos aos quais se possa legitimamente vir a ter acesso[38].

A conclusão necessária desta determinação é que a ponderação de razoabilidade de meios não se subsume apenas a uma avaliação de carácter endógeno, que se concretize na consideração da capacidade identificativa do responsável pelo tratamento em relação aos próprios meios. Uma vez que a anonimização decairá, não apenas com a recuperação plena e precisa dos dados do titular, mas também com a mera identificação, ligação ou inferência decorrente de outras fontes, tanto públicas como privadas, a robustez da anonimização estará sempre pendente de uma ponderação de carácter exógeno.

A questão é que esta aceção do conceito de identificabilidade agrava a complexidade do processo de anonimização devido à "crescente disponibilidade pública de outros conjuntos de dados"[39]. Um dos problemas clássicos na elaboração de bases de dados anónimas é a incapacidade de considerar corretamente a influência dos dados publicamente disponíveis, que podem influir decisivamente na identificação dos dados anonimizados, resultando em casos de processos de anonimização incompletos que "comportam consequências adversas, e por vezes irreparáveis, para os titulares dos dados"[40].

Desde a clássica demonstração realizada por Latanya Sweeney em 1995[41] até casos mais recentes, como a identificação de políticos alemães

---

[37] Neste sentido, o Acórdão do TJUE de 19 de outubro de 2016, Patrick Breyer v Bundesrepublik Deutschland, C-582/14, EU:C:2016:779.

[38] Neste mesmo sentido, o Acórdão do TJUE de 20 de dezembro de 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:582.

[39] Grupo de Trabalho, *op. cit.*, p. 9.

[40] *Ibid.*

[41] No contexto da sua investigação, e através da conjugação de registos médicos publicados pelo governo da Massachusetts com informação publicamente disponível, a autora logrou destacar os registos médicos do governador William Weld, utilizando elementos identificadores como o sexo, data de nascimento e código postal (os quais, igualmente, se encontravam publicamente disponíveis). Por outro lado, a própria confirmação da correta identificação do governador foi realizada mediante a contraposição dos dados obtidos com outras informações

com base em histórico de pesquisas online[42] ou a identificação de cidadãos australianos a partir da publicação de registos médicos[43], evidencia-se a existência de uma fragilidade inerente à anonimização que se encontra na possibilidade da sua conjugação com bases de dados publicamente disponíveis.

Para procurar fazer face a esta debilidade, o processo de anonimização nunca se poderá resumir à eliminação de identificadores diretos que impossibilitem a sua reversão por parte do próprio responsável. Estando assente que, em última análise, a eficácia[44] da anonimização está também dependente dos recursos identificativos de terceiro, o seu processo deverá passar, necessariamente, pela cuidada consideração, não apenas as bases de dados de carácter privado no domínio de terceiros, mas também das informações públicas que, eventualmente, possam ser imiscuídas com os dados anonimizados[45].

Torna-se, assim, evidente que existe uma universalidade de fontes de informação que deverão ser consideradas na ponderação da robustez de uma determinada anonimização. Com efeito, foi precisamente a incapacidade de considerar esta dimensão global que esteve na base do

---

públicas referentes ao mesmo (SWEENEY, Latanya. "K-anonymity: A model for protecting privacy". *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, v. 10, n.º 05, 2002, p. 557-570).

[42] Entre os exemplos discutidos na doutrina, um dos mais mediáticos é o caso da investigação levada a cabo pela jornalista Svea Eckert que, em 2016, logrou individualizar o histórico de pesquisa de políticos alemães (bem como de outras figuras públicas) com base em dados anonimizados referentes a históricos de pesquisa de 3 milhões de cidadãos alemães, aos quais teve acesso de forma gratuita.

[43] Uma equipa da universidade de Melbourne logrou realizar um exercício de identificação com base em registos médicos anónimos de 2.9 milhões de cidadãos australianos. Os referidos dados tinham sido publicados pelo departamento de saúde australiano no âmbito de uma política de transparência em agosto de 2016 sobre a premissa da sua anonimidade. Entre outros dados, o registo constava de informações referentes a diagnósticos, tratamentos e respetivos custos.

[44] Nos termos da esquematização realizada pelo Grupo de Trabalho, a eficácia de uma determinada estratégia de anonimização deverá ser aferida pela sua capacidade de impedir "que qualquer uma das partes identifique uma pessoa num conjunto de dados, relacione dois registos num conjunto de dados (ou entre dois conjuntos de dados separados) e deduza quaisquer informações desse conjunto de dados" (Grupo de Trabalho, *op. cit.*, p. 10).

[45] NARAYANAN, Arvind; FELTEN, Edward; *op. cit.*, p. 3.

caso mediático da identificação de utilizadores da plataforma Netflix[46], o qual rapidamente se tornou o exemplo paradigmático da fragilidade das técnicas de anonimização perante a abundância de dados publicamente disponíveis[47].

Como mecanismo de prevenção, e para efeitos de colmatar o risco de identificação através da associação com outras bases de dados, sugere-se a implementação de medidas integradas na família de técnicas de anonimização enquadradas na generalização. Ao aplicar medidas particulares de agregação, como o K-anonimato[48], estas abordagens teriam o condão de generalizar ou diluir os atributos dos titulares dos dados, complexificando a identificação, mesmo com o recurso a outras fontes de informação. No entanto, existem investigações que reportam que as garantias que outrora pudessem ter sido prestadas pela generalização (no âmbito de uma conjetura na qual prevaleciam bases de dados de cariz unidimensional) deixou de se verificar no panorama atual do tratamento de dados pessoais. Uma vez que proeminam hoje as bases de dados de cariz complexo[49], refere-se que a abundância de informação publicamente

---

[46] NARAYANAN, Arvind; SHMATIKOV, Vitaly. "Robust de-anonymization of large sparse datasets (How to break anonymity of the Netflix prize dataset)", *IEEE Symposium on Security and Privacy, 2008, p. 111-125,* Disponível em: https://www.semanticscholar.org/paper/How-To-Break-Anonymity-of-the-Netflix-Prize-Dataset-Narayanan-Shmatikov/56116e8ce3f57bec578ac60f6d68333aea5af59e, acedido a: 21.04.2019.

[47] Em 2 de outubro de 2006, a provedora global de filmes e séries de televisão via *streaming* Netflix promoveu um concurso tendente à elaboração de um algoritmo que promovesse a sua recomendação de filmes. Para efeitos operativos, a empresa publicou informação referente a 100.480.507 avaliações realizadas por 480.189 dos seus subscritores no período compreendido entre dezembro de 1999 e dezembro de 2005. O processo de anonimização foi feito através da remoção de informação passível de identificação direta dos subscritores. Contudo, utilizando como fonte de informação adicional os dados publicamente disponíveis no site *Internet Movie Database* (conhecido como "*IMDb*"), demonstrou-se que era possível estabelecer uma conexão entre os registos e os subscritores, contornando os esforços de anonimização.

[48] As técnicas de agregação, nas quais o k-anonimato se insere, procuram impedir que o titular seja identificado através da sua agregação com outros sujeitos que partilham um elemento geral comum. A particularidade do k-anonimato reside no facto de que pretende assegurar que nesse agrupamento exista, pelo menos, um determinado número de titulares, no sentido de evitar a individualização de um sujeito em particular.

[49] ZIBUSCHKA, Jan, *et al., op. cit.*, p. 4.

disponível coloca em causa a proteção garantida pela anonimização[50], mesmo no caso de bases de dados anonimizadas com uma elevada taxa de generalização[51].

A conclusão que devemos retirar desta conjetura é que a abundância de informações livremente disponibilizadas (incluindo as que são promovidas pelos próprios titulares no âmbito do ecossistema digital) promove, necessariamente, a individualização da população com o aumento dos atributos disponíveis[52]. Como tal, a probabilidade de identificar um indivíduo é alta, o que acaba por comprometer o nível de proteção assegurado pela redução da individualidade dos dados. Perante estas limitações, a doutrina vem defender que a anonimização eficiente de determinado tipo de dados pessoais, mais do que uma dificuldade técnica, representa-se como uma efetiva impossibilidade prática[53], chegando-se a falar de uma verdadeira quebra de confiança na anonimização enquanto meio de tutela de dados pessoais.

2.2.2. Influência de elementos de carácter intrínseco: O impacto da natureza dos dados na viabilidade da anonimização

Embora concebamos que uma das principais limitações do processo de anonimização poderá ser encontrada no contexto no qual este se

---

[50] ROCHER, Luc, *et al., op. cit.*, p. 10.

[51] Ainda assim, porém, encontramos argumentos que defendem que, desde que seja realizada uma correta implementação de técnicas de anonimização, mesmo quando se logra reverter o respetivo processo, permanece sempre um determinado grau de incerteza. Assente neste nível de dúvida, alega-se que seria possível ao titular da informação sonegar a sua representação nos dados evidenciados, o que, em última análise, poderia representar um reforço na tutela do sujeito identificado. Contudo, estudos recentes vêm rebater este tipo de argumentação, tendo-se logrado desenvolver modelos que apontam para a existência de um alto grau de probabilidade de que o resultado de tarefas de reversão sejam representações corretas dos dados reais (ROCHER, Luc, *et al., op. cit.*, p. 1-5).

[52] GOLLE, Philippe. *Revisiting the Uniqueness of Simple Demographics in the US Population*. Palo Alto Research Center, 2006, p. 1, disponível em: https://www.privacylives.com/wp-content/uploads/2010/01/golle-reidentification-deanonymization-2006.pdf., acedido a: 14.05.2018.

[53] ZIBUSCHKA, Jan. *et al*, *op. cit.*, p.71.

enquadra[54], a verdade é que a avaliação casuística exigida pelo critério da razoabilidade demanda, claramente, uma análise cuidada do tipo de dados que se pretende anonimizar. Uma vez que cada técnica de anonimização possui debilidades que lhe são inerentes, e tendo em conta que não existe um caminho pré-determinado para descortinar objetivamente quais as medidas exatas a implementar, a sua eventual adequação ao caso concreto dependerá sempre das particularidades dos dados em causa[55].

Aliás, do nosso ponto de vista, julgamos poder encontrar uma relação direta entre a evolução destas especificidades ao longo do tempo e o declínio do nível de eficiência das técnicas de anonimização. Nomeadamente, num contexto de limitada capacidade de processamento de informação, como o que se verificava outrora, no qual predominava um tratamento desprovido da complexidade multidimensional da atualidade, as técnicas tradicionais de anonimização poderiam, efetivamente, representar maiores garantias, uma vez que seria mais simples proceder à generalização dos seus atributos. Contudo, a atualidade é caracterizada pela proliferação das bases de dados de cariz complexo, maioritariamente compostas pela denominada *high-dimentional data*[56], e no âmbito da qual se evidencia um claro limite quanto à medida de generalização de que determinados dados podem ser alvo sem que se comprometa gravemente a sua integridade.

Devido à elevada taxa de individualização[57] das informações tratadas hoje em dia, investigações recentes procuram demostrar que a

---

[54] ELLIOT, Mark. *et al*, *op. cit.*, p. 67.

[55] Grupo de Trabalho, *op. cit.*, p. 28.

[56] Na sua essência, este conceito refere-se às informações constituídas por uma grande quantidade de elementos identificadores para cada indivíduo, de tal forma que os registos individuais possuem uma grande probabilidade de serem únicos e diferentes dos demais registos (neste sentido, ZIBUSCHKA, Jan, *et al.*, *op. cit.*, p. 4).

[57] A dificuldade na anonimização deste tipo de dados está intimamente ligada aos traços característicos do comportamento humano. Nomeadamente, num conjunto de dados anónimos, os movimentos pendulares diários permitem assumir, com um certo nível de segurança, que determinados pontos representam o local trabalho e a residência de uma dada pessoa. Como tal, os dados de localização têm uma grande singularidade. Em determinados estudos, chega-se a referir que perto de 95% de rastreios, compostos por quatro locais, tem um carácter único (neste sentido, MONTJOYE, Yves-Alexandre; HIDALGO, César A.; VERLEYSEN, Michel; BLONDEL, Vincent. "Unique in the Crowd: The privacy bounds of human mobility". *Scientific Reports*, v. 3, n.º 1376, p. 1-5, disponível em: https://www.nature.com/articles/srep01376, acedido a: 21.05.2019).

anonimização de determinados dados de cariz complexo (como seja a generalidade dos dados referentes a rastreamentos de dispositivos de comunicação[58], os dados referentes às redes sociais[59], determinados registos médicos ou dados comportamentais em geral[60]) poderá consubstanciar um desafio efetivamente intransponível[61]. Por outro lado, se considerarmos ainda a mencionada possibilidade de conjugação deste tipo de dados com o crescente acervo de informação livremente disponível, facilmente se antevê a provável extrapolação do risco de identificação.[62]

Ou seja, além de representar um elemento de complexificação da tarefa exigida ao responsável pelo tratamento, a consideração das particularidades dos dados a tratar reveste-se de particular importância, uma vez que, em última análise, poderá comprometer a própria viabilidade efetiva da anonimização.

2.3. O carácter antagónico das finalidades visadas pelo processo de anonimização

2.3.1. A minimização do risco residual

À parte de quaisquer considerações relativas ao sucesso efetivo deste processo, a anonimização traduz-se, acima de tudo, num mecanismo de tutela do direito fundamental à proteção de dados pessoais. Nesta medida, a sua finalidade principal concretiza-se num esforço de pendor preventivo que se concentra na proteção efetiva dos direitos do titular.

Conforme esquematizado pelo Grupo de Trabalho, esta finalidade seria lograda se a anonimização conseguisse impedir que, com base em certos

---

[58] MONTJOYE, Yves-Alexandre, *et al.*, *op. cit.*

[59] UGANDER, Johan; KARRER, Brian; BACKSTROM, Lars; MARLOW, Cameron. "The Anatomy of the Facebook Social Graph.", 2011, disponível em: https://arxiv.org/abs/1111.4503, acedido a: 22.10.2019.

[60] ZIBUSCHKA, Jan, et al., op. cit., p. 76.

[61] NARAYANAN, Arvind. *et al*, *op. cit.*, p. 1.

[62] NARAYANAN, Arvind. *et al*, *op. cit.*, p.2.

dados, fosse possível qualquer identificação[63], ligação[64] ou inferência[65] em relação aos respetivos titulares. No entanto, e conforme resulta patente dos considerandos do RGPD, não se exige que essa finalidade seja lograda em termos absolutos. Ou seja, não é exigível ao responsável que o risco de identificação, ligação ou inferência seja reduzido à nulidade.

Partindo destes pressupostos, o legislador europeu parece compreender e aceitar o facto de que não existem técnicas de anonimização que disponibilizem uma resposta cabalmente satisfatória a esta questão[66]. Embora lhes seja reconhecido um grau variável de adequação consoante as circunstâncias concretas, as investigações levadas a cabo nesta área revelam sistematicamente que nenhuma técnica é, por si só, desprovida de lacunas[67]. É partindo desta perspetiva que a legislação europeia abraça um conceito lato de anonimização, o qual se encontra apto a compreender e tolerar a permanência de um fator de risco inerente ao dado anonimizado[68]. Trata-se de um risco de carácter necessariamente residual, cuja eliminação representaria uma condição inexigível ao responsável pelo tratamento, uma vez que o seu aproveitamento para efeitos de identificação seria desrazoável (tendo em conta os meios disponíveis).

---

[63] Nos termos do referido pelo Grupo de Trabalho, a identificação ocorrerá quando seja possível "isolar alguns ou todos os registos que identifiquem uma pessoa num conjunto de dados" (Grupo de Trabalho, *op. cit.* p. 3). Em concreto, existirá o risco de identificação quando for possível individualizar o titular dos dados, mesmo após a conclusão do processo de anonimização.

[64] O risco de ligação corresponde à possibilidade de se determinar uma relação entre os registos referentes a um mesmo titular. Relativamente a este aspeto, o Grupo de Trabalho vem alertar para o facto de que uma técnica poderá ser efetiva contra a identificação, mas, ainda assim, ser ineficaz contra o risco de ligação. Isto sucederá quando uma determinada técnica de anonimização logre coartar o destacamento do indivíduo num determinado grupo, porém, seja ainda possível determinar que um grupo de dados se refere a um mesmo grupo de pessoas (Grupo de Trabalho, *op. cit.* p. 3).

[65] Ainda nos termos do avançado pelo Grupo de Trabalho, fundamentalmente, a inferência refere-se à "possibilidade de deduzir (...) o valor de um atributo a partir dos valores de um conjunto de outros atributos". Devido à natureza deste conceito, a possibilidade da sua verificação estará sempre pendente de uma avaliação de probabilidade na eventual concretização efetiva das informações inferidas (Grupo de Trabalho, *op. cit.* p. 3).

[66] Grupo de Trabalho, op. cit., p. 9.

[67] *Ibid.*, p. 13.

[68] *Ibid.*, p. 7.

A contraposição necessária desta construção implica que o risco não possa exceder o carácter residual. Caso tal se verifique, o processo de anonimização deverá ser considerado débil, uma vez que o respetivo risco ultrapassa o critério da razoabilidade, pelo que os dados produzidos pelo mesmo não possuirão a natureza de dado anonimizado.

Desonerado da responsabilidade da eliminação absoluta do risco, ao responsável pelo tratamento é, porém, exigido que encete todos os meios razoavelmente disponíveis para a sua minimização. É sobre esta premissa que o responsável pelo tratamento deverá avaliar a conjugação das técnicas de anonimização a utilizar[69]. Cada vez mais, a doutrina tem evidenciado que uma das falhas correntes das práticas atuais de anonimização se encontra na aplicação destas técnicas sem ter em conta a sua efetividade no caso concreto (ou mesmo o impacto que o procedimento possa ter nos próprios dados)[70]. Uma vez que as diversas técnicas de anonimização possuem benefícios e limitações próprias[71], torna-se essencial realizar uma ponderação casuística que se centre na efetividade concreta das técnicas de anonimização, avaliando a pertinência de eventuais combinações de técnicas no sentido da sua complementação[72].

Devido à natureza dinâmica dos elementos contextuais que influem sobre a efetividade da anonimização, devemos salientar que a minimização do risco residual não é uma condição estática e exige uma ponderação contínua de carácter preventivo. O responsável pelo tratamento deverá assegurar-se que o nível de risco se mantém, efetivamente, residual ao longo do tempo[73].

2.3.2. A maximização da utilidade residual

Sem nos desviarmos das premissas alcançadas até este ponto, e muito embora a proteção dos direitos do titular dos dados assuma um papel

---

[69] PANG, Ruoming; ALLMAN, Mark; PAXSON, Vern; LEE, Jason. "The Devil and Packet Trace Anonymization". *ACM SIGCOMM Computer Communication Review*, 36. p. 29-38, disponível em: https://www.icir.org/enterprise-tracing/devil-ccr-jan06.pdf, acedido a: 22.08.2019.

[70] NALDI, Maurizio, *op. cit.*

[71] Grupo de Trabalho, op. cit., p. 26.

[72] *Ibid.*

[73] NARAYANAN, Arvind. et al, op. cit., p. 5.

epicêntrico nesta matéria, devemos manter presente que a minimização do risco residual não se afigura como o único objetivo do processo de anonimização[74].

Adensando a complexidade que reveste este processo, através de uma abordagem eminentemente pragmática, a doutrina tem procurado realçar que a minimização do risco representa apenas um dos vértices deste problema[75]. Como é obvio, todo o tratamento de dados pessoais que vise a sua anonimização, além da proteção dos titulares, tem sempre em vista a sua futura utilização[76]. No sentido de promover essa finalidade, além da existência do risco residual, o responsável pelo tratamento deverá considerar também o nível de utilidade que os dados conservarão após o processo de anonimização[77]. É precisamente nesta dicotomia que se encontra o paradoxo que complexifica o processo de anonimização no plano das suas finalidades[78].

Conceptualmente, e para efeitos de exposição, seria possível conceber um processo de anonimização *stricto sensu* que, ao deturpar completamente a informação, lograsse impedir categoricamente a recondução de quaisquer valores aos respetivos titulares e vice-versa. Evidentemente, este ponto representaria um nível máximo de anonimização e, consequentemente, de proteção do titular dos dados. Tal adulteração, porém, traduzir-se-ia num nível mínimo (ou nulo) de utilidade dos dados tratados, uma vez que esse tratamento colocaria em causa a fidelidade – e consequente utilidade – dos mesmos[79]. Inversamente, dados originais, ou sujeitos a um procedimento débil de anonimização, embora representem um alto nível de utilidade (uma vez que não se afastariam dos valores originais) traduziriam um nível de anonimização mínimo ou inexistente[80]. Perante este contraste, e se tivermos presente que não é incomum que o principal

---

[74] BAMBAUER, Jane; MURALIDHAR, Krishnamurty; SARATHY, Rathindra. "Fool's Gold: An Illustrated Critique of Differential Privacy". *Vanderbilt Journal of Entertainment and Technology Law*, 16, n.º 4, 2014, p. 701-755, disponível em: http://www.jetlaw.org/wp-content/uploads/2014/06/Bambauer_Final.pdf, acedido a: 26.08.2019.

[75] NALDI, Maurizio, *op. cit*.

[76] ELLIOT, Mark. *et al, op. cit*., p. 18.

[77] Grupo de Trabalho, *op. cit*., p. 4.

[78] ZIBUSCHKA, Jan, *et al*., *op. cit*., p. 71.

[79] *Ibid*., p. 55.

[80] ZIBUSCHKA, Jan. *et al*, *op. cit*., p.76.

elemento de risco de uma determinada base de dados seja precisamente o fator de maior utilidade, facilmente se antevê a dificuldade que esta conformação representa[81].

Torna-se evidente, assim, que esta correlação demanda um equilíbrio próprio, cuja ponderação deverá assumir um papel fulcral no processo de anonimização[82], pois, da sua frustração, poderá decorrer a futilidade de todo o processo, quer seja pela inutilização dos dados tratados ou pela ineficácia das medidas implementadas.

A natureza pragmática da questão condiciona a sua avaliação a um critério necessariamente casuístico e virado para as finalidades específicas do caso, porém, para efeitos de esquematização da lógica que deverá orientar esta consideração, podemos afirmar que, independentemente das particularidades da questão em concreto, o responsável deverá sempre procurar almejar um ponto de equilíbrio[83]. Uma vez que o incremento num dos ideais comporta, necessariamente, um prejuízo para o outro, entendemos que a conformação de uma estratégia de anonimização torna essencial procurar um ponto que, por um lado, procure evitar ao máximo os riscos identificados *supra* e, por outro, procure ainda assegurar um máximo de utilidade. Apesar de que, na prática, este patamar seja virtualmente impossível de antever, em termos teóricos, será possível conceber, em torno deste ponto, um espaço de razoabilidade a nível do risco e da utilidade que logre satisfazer o conceito *lato sensu* consagrado no âmbito da legislação europeia.

Não deixa de ser evidente, porém, que esta avaliação estará sempre revestida de uma índole necessariamente subjetiva e casuística que lhe confere uma dimensão de fragilidade que, por sinal, desafia a efetividade da maior parte das técnicas de anonimização. Ilustrativamente, poderíamos indicar a implementação de mecanismos baseados na

---

[81] ELLIOT, Mark. *et al, op. cit.*, p. 41.

[82] NALDI, Maurizio, op. cit.

[83] Para efeitos de ilustração do raciocínio vertido, fazemos referência à lei da eficiência de Pareto, desenvolvida pelo economista Vilfredo Frederico Damaso Pareto, na sua obra Cours d`Économie Politique de 1897. Em termos simplistas, este conceito pretende representar uma conjetura na qual se procede à alocação de recursos de forma a que não se vislumbre uma outra organização de recursos viável que possa promover nenhum dos interesses sem que, em contrapartida, se implique um prejuízo para o outro.

privacidade diferencial[84] como a procura de soluções de compromisso para esta relação dicotómica[85]. Tratando-se de um método dinâmico de particularização do nível de distorção dos dados ao caso específico da sua consulta, este mecanismo providenciaria uma relação equilibrada entre o risco e a utilidade. Contudo, a verdade é que não presta uma resposta definitiva a esta questão. Importa recordar que, além das limitações que lhe são comumente imputadas[86], no seu esforço por prestar uma solução de equilíbrio entre as duas finalidades, esta técnica acaba por sacrificar a natureza anónima dos dados que produz. Uma vez que favorece a preservação de uma versão original dos dados, mesmo após a implementação deste mecanismo, mantém-se uma via concreta para a identificação dos titulares. Como tal, os dados sujeitos a esta técnica não poderão ser considerados aquém do âmbito material do RGPD e, nesta medida, pelo menos na iteração atual dos contornos desta técnica, ainda não logra representar uma resposta definitiva à questão da proteção de dados mediante a anonimização.

Indo além das limitações próprias das diversas técnicas de anonimização, devemos também realçar que a natureza da informação poderá dificultar a procura por uma relação de equilíbrio. Torna-se hoje comum

---

[84] WOOD, Alexandra; ALTMAN, Micah, BEMBENE, Aaron; BUN, Mark; GABOARDI, Marco; HONAKER, James; NISSIM, Kobbi; O´BRIEN, David; STEINKE, Thomas; VADHAN, Salil. "Differential privacy: A primer for a non-technical audience.", *Vanderbilt Journal of Entertainment & Technology Law*, 21, n.º 1, 2018, p. 209-275, disponível em: http://privacytools.seas.harvard.edu/files/privacytools/files/pedagogical-document-dp_0.pdf., acedido a: 26.08.2019.

[85] Considerada como um passo em frente em relação à proteção de dados e à tutela da privacidade, esta técnica desenvolve as soluções baseadas na adição de ruído, procurando, ao mesmo tempo, promover a preservação da utilidade dos dados. Em lugar de imbuir uma medida pré-determinada de distorção à informação, esta técnica conserva uma cópia dos dados originais e se limita a aplicar um certo nível de ruído apenas aos resultados visualizados pelo sujeito que procede à consulta da base de dados. Em suma, trata-se de um mecanismo particularizado e especializado ao terceiro que a consulta, permitindo uma contínua adaptação à necessidade de adição de ruído.

[86] Tal como sugere o grupo de trabalho, através do acesso contínuo à base de dados, eventualmente por um conjunto diferenciado de indivíduos, seria conceptualmente possível retirar informação que permita a identificação, ligação ou inferência sobre alguns dos titulares. Muito embora o enquadramento dos dados como dados pessoais lograsse manter as garantias aos titulares, não se poderá considerar que estejam ultrapassados os riscos elencados *supra*.

encontrar contributos científicos que evidenciam que, no âmbito do tratamento de determinado tipo de dados, a minimização do risco a um nível razoavelmente satisfatório implica sempre uma desmedida distorção dos mesmos, prejudicando incontornavelmente a sua utilidade[87]. Principalmente no âmbito de dados complexos, nos quais existe um número considerável de quase-identificadores, a limitação do nível de generalização que poderá ser efetuada sem comprometer a utilidade dos dados é alta[88]. Nesta medida, chega-se mesmo a referir que, em relação a determinados tipos de dados, um processo de anonimização com um alto índice de utilidade e segurança é uma impossibilidade fáctica[89].

É nas complexas nuances deste equilíbrio que se desenvolvem as principais dúvidas quanto à virtude da anonimização enquanto meio de proteção de dados pessoais[90]. Na medida em que assenta na premissa questionável da possibilidade de obter dados úteis e, ao mesmo tempo, verdadeiramente anonimizados[91], pondera-se a necessidade efetiva de uma mudança de paradigma que se afaste da anonimização e se foque na transparência e numa lógica de responsabilidade[92].

Considerações finais

Tal como procurámos antecipar na introdução do presente texto, muito embora a proteção de dados pessoais se revele como um direito fundamental amplamente reconhecido em termos globais (embora em diferentes níveis), os seus contornos são constantemente moldados e desafiados pelo desenvolvimento da tecnologia da informação[93], a qual medra num ritmo distinto do que a capacidade de adaptação das soluções jurídicas, representando um especial desafio para os esforços regulatórios.

---

87 BAMBAUER, Jane. *et al, op. cit.*, p 703.
88 NARAYANAN, Arvind. *et al, op. cit.*, p. 7.
89 MURAKAMI, Takao. *et al, op. cit.*
90 ELLIOT, Mark. *et al, op. cit.*, p. 18.
91 OHM, Paul., *op. cit.*, p. 1704.
92 ZIBUSCHKA, Jan, et al., op. cit., p 79.
93 *Ibid.*, p.71.

Assente nas considerações tecidas até este momento, entendemos que a viabilidade prática de um processo de anonimização está pendente de um equilíbrio, necessariamente ténue, entre a utilidade e o risco residual[94] que, em última análise, se encontra nas mãos do próprio responsável pelo tratamento e cuja resiliência depende da ponderação de uma universalidade de fatores que lhe são alheios[95], como a conjetura contemporânea dos recursos tecnológicos e a disponibilidade de informação que os próprios titulares continuamente disseminam. Permitimo-nos, assim, questionar a viabilidade de um regime assente numa ponderação de razoabilidade de meios. Já de si um conceito indeterminado, este critério poderá consagrar-se como uma realidade indeterminável se considerarmos o seu efetivo enquadramento prático.

Por um lado, o processamento de informação encontra-se enquadrado num contexto dinâmico que promove uma constante evolução de meios e recursos que impossibilita a antevisão do que poderá ser considerado concebível a curtíssimo prazo. Por outro lado, conforme também observámos, a doutrina revela como uma crescente fonte de informações publicamente disponibilizadas compromete a efetividade das técnicas de anonimização. A questão é que a dificuldade deste processo não se traduz necessariamente numa maior proteção do titular. O que os casos de estudo têm demostrado é que a complexidade da sua ponderação tem resultado na produção de dados ilusoriamente anonimizados que promove a vulnerabilidade dos titulares.

Assim sendo, entendemos que, por se compaginar na realidade volátil e mutável do ecossistema digital e tecnológico, o critério da razoabilidade de meios poderá encontrar-se vazio de conteúdo, uma vez que poderá ser impossível determinar o que é, num dado momento, efetivamente razoável e, em última análise, poderá contribuir para o desenvolvimento de um ambiente de incerteza por parte dos responsáveis pelo tratamento e de desconfiança por parte dos titulares dos dados.

Transpondo a nossa objetiva ao regime consagrado pela União aos dados anonimizados, observamos como estas considerações nos levam a suspeitar que na delicada ponderação de razoabilidade se encontra pendente a possibilidade de sonegação dos mais básicos direitos e deveres

---

[94] ELLIOT, Mark. *et al*, *op. cit.*, p. 19.

[95] *Ibid.*, p. 16.

decorrentes do RGPD. Neste sentido, julgamos que seria, efetivamente, defensável uma mudança de paradigma a nível da tutela dos dados anónimos ou do próprio conceito de anonimização[96].

Conforme é nosso entendimento, o enquadramento legislativo europeu referente à proteção de dados encara o resultado do processo de anonimização de dados pessoais em termos equiparados ao efetivo apagamento dos mesmos. Salvo exceções técnicas e recursos de recuperação de informação, em princípio, um dado apagado estará objetivamente inacessível. No caso da anonimização, como vimos, a reidentificação do titular não é uma impossibilidade objetiva, na medida em que está pendente de um juízo de razoabilidade eminentemente subjetivo. Esta fragilidade, bem como a dimensão omnipresente de risco que inerentemente comporta, não é coerente com esta equiparação. Como tal, entendemos que a consagração de um regime jurídico como o que se verifica à luz da atual legislação europeia apenas se justificaria no contexto de uma conceção absoluta ou *strito sensu* de anonimização[97].

Ao aceitar-se a impossibilidade fáctica de tal realidade, consideraríamos coerente revestir o processo de anonimização *lato sensu* de um núcleo básico de garantias. A título meramente exemplificativo, e admitindo a necessidade de maturação da presente construção, se, efetivamente, o processo de anonimização comporta sempre um risco para o respetivo titular, não se poderia aceitar a conclusão de que este tratamento pudesse ter lugar sem o assentimento ou intervenção deste último[98].

---

[96] ZIBUSCHKA, Jan, *et al., op. cit.,* p. 72.

[97] *Ibid*., p. 78.

[98] Com efeito, e uma vez que os dados pessoais permanecerão sob a tutela do RGPD até que sejam sujeitos ao processo de anonimização, este tratamento (conforme definido pelo n.º 2 do art. 4.º do RGPD) deverá ser realizado em observância do princípio da licitude [consagrado na alínea a) do n.º 1 do art. 5.º do RGPD]. Contudo, o responsável poderá invocar qualquer um dos fundamentos de licitude previstos nas várias alíneas do n.º 1 do art. 6 do RGPD, não estando limitado ao consentimento. Mais, se observarmos ainda que este tratamento não contraria necessariamente os vetores do princípio da limitação das finalidades [consagrado na alínea b) do n.º 1 do art. 5.º do RGPD] – uma vez que o mesmo, em princípio, poderá ser considerado compatível com a finalidade para a qual os respetivos dados foram originalmente recolhidos –, torna-se evidente que o processo de anonimização poderá tecnicamente desenrolar-se de forma alheia aos titulares dos dados (neste sentido Grupo de Trabalho, op. cit., p. 8).

Muito embora, em termos conceptuais, o processo de anonimização vise representar uma mais-valia para a proteção do titular dos dados, a existência de um nível de risco constante (bem como o facto de que este processo poderá coartar os direitos e deveres constantes do RGPD), implica que o interesse legítimo do responsável pelo tratamento não possa ser considerado, *à priori*, elemento suficiente para encetar a anonimização[99]. Em nome da transparência, e para efeitos da proteção dos direitos do titular dos dados, consideramos que o processo de anonimização careceria de comprovação de que o mesmo tem consciência do nível de risco e o aceita como tal. Ou seja, deverá reconhecer-se a fragilidade da anonimização e promover a implementação de uma correta política de transparência e consentimento[100].

Nesta mesma linha de raciocínio, seria também defensável a concretização do princípio da necessidade ao processo de anonimização. Na prática, atendendo à omnipresença do referido fator de risco, o responsável pelo tratamento não deverá apenas provar que considera as expectativas dos titulares neste processo, mas também demostrar a concreta necessidade de optar pela anonimização e conservação dos dados, em lugar de proceder à efetiva eliminação dos mesmos.

Seria, nesta medida, de ponderar, como tem acontecido na literatura recente[101], a possibilidade de repensar a abordagem consagrada à

---

[99] Por sinal, deverá salientar-se que, muito embora o consentimento pudesse ser equacionado como fundamento por excelência em nome da transparência, a doutrina especializada tem defendido que, para efeitos de anonimização, o consentimento poderá revelar-se contraproducente (EMAM, Khaled El; HINTZE, Mike. *Does anonymization or de-identification require consent under the GDPR?,* 2019, disponível em: https://iapp.org/news/a/does-anonymization--or-de-identification-require-consent-under-the-gdpr, acedido a: 14.02.2019). Nos termos deste entendimento, além de ser difícil de requerer no âmbito do processamento de *big data* ou no contexto da aprendizagem automática (*machine learning*), o consentimento do titular, para tais efeitos, poderia corromper determinados resultados devido à sua índole tendenciosa. Conforme defende esta abordagem, os titulares que aderem ao tratamento, possuem um perfil tendencialmente semelhante, o que, ao excluir os que não consentiriam, poderia subverter a fidelidade dos dados. Como tal, defende-se que, no contexto da anonimização de dados, a legitimação da anonimização através do interesse legítimo [nos termos da alínea f) do n.º 1 do art. 6.º do RGPD] poderia revelar-se mais pertinente do que a concentração no consentimento do titular.

[100] ZIBUSCHKA, Jan, *et al., op. cit.,* p. 79.

[101] *Ibid.*, p. 72.

anonimização, revestindo-a de uma tutela coerente com os objetivos consagrados no âmbito da estratégia europeia para o mercado único europeu que, no seio dos seus principais baluartes, consagra o desenvolvimento da confiança no quadro do ecossistema digital.

Two years in: Does the GDPR already need updates? *A question brought by algorithmic decision-making*

Beatriz Santiago Trindade*

Resumo: Hoje, mais do que em outro momento, vive-se uma (r)evolução tecnológica constante. Numa altura em que os dados pessoais são perspetivados como bens transacionáveis, valiosíssimos, também já referidos como "o novo petróleo", cumpre-nos verificar se, num contexto determinado, os textos legislativos neste âmbito providenciam uma proteção adequada. Estaremos, porventura, a ser excessivamente cautelosos a apontar para a necessidade de alterar o Regulamento Geral de Proteção de Dados? Ou será que a solução cabe apenas às entidades que desenvolvem as novas tecnologias de Inteligência Artificial?

Palavras-chave: *Proteção de Dados; Inteligência Artificial; Machine Learning; Dados Pessoais; Algoritmos*

Abstract: Nowadays, more than ever, we live a constant technological (r)evolution. And, today, in a time when personal data are prospected as very valuable "exchange" goods, hence already called "the new oil", it is up to us the need to certify ourselves whether present legislative texts are able to provide an adequate protection to it. Or are we already, perhaps in a very cautious way, facing the necessity to update the General Data Protection Regulation? Maybe the solution lies with the entities that develop the new Artificial Intelligence technologies...?

Keywords: *Data Protection, Artificial Intelligence; Machine Learning; Personal Data; Algorithms*

---

* Licenciada em Direito pela Faculdade de Direito da Universidade de Coimbra. Mestre em Direito Internacional e Europeu pela Faculdade de Direito da Universidade Nova de Lisboa. DPO certificada pelo Centro Europeu de Privacidade e Cibersegurança da Faculdade de Direito de Maastricht.

Introduction

Nowadays, there is absolutely no doubt that technology is all around us. It is in our house, our cars, our streets, through the use of internet, computers and other technologies, such as Internet of Things (IoT). Tech devices are practically omnipresent, namely in fields like Health, Finance or Education. The machines are mostly fed through data that us, Humans, insert in them, learning through the complex algorithms how to analyse data sets and make predictions based on them.

The technology we use has, in its inner workings, lots of mechanisms, namely *Machine Learning* and *Artificial Intelligence*[1], which works through the work of hand-coding the solution to each problem (for example, that can be helping someone going from A to B or translating text between two or more different languages). To better explain this, one shall first acknowledge that the machines collect and process big amounts of data, and amongst those data, there are personal data[2].

The machines achieve the solution which they are confronted by analysing the data we feed them and then finding patterns between those data. Through these actions, one tends to think there isn't any (human) bias. Nevertheless, it is urgent to remember that, by the sole use of data, the machine is not necessarily neutral.

Even with the best intentions, it is very difficult, if not practically impossible, to separate the developer from his/her own bias, which are inherent to every human being. Inevitably, our own human bias is transferred to the machine (well, mostly algorithms and software), since the idea that humans are biased by nature is supported by some

---

[1] Through the use of the terms of *Machine Learning*, as well as *Artificial Intelligence*, one pretends to refer to systems based on decision-making algorithms. In this sense, the machines are mainly used to help reach a decision or formulate some kind of recommendation for action. In short, we are going to analyze how decisions reached by a machine can affect its users, while also taking into account that data protection is, in its own nature, a fundamental right and has to be, therefore, balanced against many other fundamental rights that are established by the Charter of Fundamental Rights of the European Union (CFREU).

[2] Council of Europe, *"Handbook on European data protection law – 2018 edition"*, Luxembourg: Publications Office of the European Union, 2018, p. 347. Also available online <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf>. Consulted on 15 October 2019.

authors[3]. Biases are often seen a form of optimizing the brain functions and have their root in individual experiences, as well as the social and cultural environment in which an individual is inserted[4].

This can be seen as a very complex issue, since technology must serve everyone. So the machine may "suffer" from different kinds of biases[5], such as interaction bias[6], latent bias[7] and selection bias[8].

The bigger question we now face is: as we develop more and more technology to make our lives better or easier, how do we keep our biases out of the algorithms we create, whilst protecting the data from numerous data subjects for the construction of the machine's sample?

Considering the aforementioned human bias, are the machines also necessarily (and/or inevitably) biased? And how does our legislation, namely the EU General Data Protection Regulation (GDPR)[9], keep our rights safe[10]?

---

[3] MOSKOWITZ, Gordon, *Are we all Inherently biased?*, Lehigh University. Article available in: https://www1.lehigh.edu/research/consequence/are-we-all-inherently-biased. Consulted on 12 February 2020.

This Author is quite clear when defending this idea: "(...) While I would say "no" to the question of whether stereotyping is inevitable, I would answer in the affirmative to the question of whether people are inherently biased. I see all human thought and action on the environment as always in the service of the goals of the person within that environment. These goals may be invisible to the naked eye, implicit (unconscious). But we are always pursuing a goal with every action, with every thought. Thus every action and thought is biased by these goals. (...)"

[4] XIANG, Mark (2019), *Human Bias in Machine Learning – What it means in our modern big data world*. Towards Data Science. Retrieved from https://towardsdatascience.com/bias-what-it-means-in-the-big-data-world-6e64893e92a1. Consulted on 12 February 2020.

[5] To understand this, the visualization of this short clip is advised: https://www.youtube.com/watch?v=59bMh59JQDo. These are not the only biases present in Machine Learning mechanisms, though.

[6] The algorithm becomes biased by the way the user interacts with it.

[7] These types of biases are mainly related with elements such as gender, income, race, or other characteristics.

[8] Selection bias happens when an algorithm favours one population or segment of population, at the expense of other subjects.

[9] Regulation (EU) 2016/679 of the European Parliament and of The Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[10] Cfr. DREYER, Stephan, SHULZ, Wolfgang, *The GDPR and algorithmic decision-making-Safeguarding individual rights, but forgetting society*. Völkerrechtsblog – International Law &

Despite the unquestionable benefits[11] brought by technologies designed with the intent of making our lives better and easier, one cannot forget that in order for those technologies to function properly or as intended, a feed of our data is needed[12]. Errors or bias, not only among the collected and shared data, but also in the – or as a result of the – automated decision-making process, can lead to inaccurate classifications, assessments based on imprecise projections and a negative impact on individuals[13].

It is not excessive to recall we are dealing with fundamental rights, and, therefore, worthy of the highest protection possible.

The present paper aims to confront the reader with the possible obstacles new technology poses to the community, whilst trying not to disregard the real benefits these innovations give us. It does not pretend to give a close answer to the general problem of automated decision-making, but at least bring the question to present minds as they assist to newer and more complex developments on this particular field.

Does the solution lie in the beginning of the process, when we insert data in the machines and work the algorithms out, or, on the contrary, it resides in the aftermath, the legislation that regulates the use that tech makes out of our data?

International Legal Thought, 2019. Retrieved from https://voelkerrechtsblog.org/the-gdpr-and-algorithmic-decision-making/. Consulted on 15 October 2019.

[11] For example, in the beginning of the new Corona virus (nCov-2019) outbreak, a Canadian health monitoring platform alerted to the possibility that an epidemy was about to begin. BlueDot uses an AI-algorithm that analyses and combines foreign language news reports and animal and plant networks, which ultimately led to the conclusion that the outbreak was about to take place. https://www.wired.com/story/ai-epidemiologist-wuhan-public-health-warnings/amp?fbclid=IwAR2LqZc2UB3DtDg-ccYPHuBzmB-voCOyFPp02nWuaELkJHstFupuExZhgYY. Consulted on 08 February 2020).

[12] Council of Europe, *"Handbook on European data protection law – 2018 edition"*, Luxembourg: Publications Office of the European Union, 2018, p. 347

[13] Article 29 Data Protection Working Party (W29), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* Adopted on 3 October 2017 and last revised and adopted on 6 February 2018, page 27.

1. The relation between Artificial Intelligence (in general) and the GDPR

EU GDPR adopts a risk based approach towards data protection, and it is very easy to understand why: we are dealing with fundamental rights and, as one can infer from reading the Charter of Fundamental Rights of the European Union (2012/C 326/02), these rights must be balanced against each other.

GDPR focuses on the personal/individual dimension of the (data) subject, while Artificial Intelligence focuses more on the collective/group dimension. So, in a way, GDPR presents itself as inadequate for AI regulation. But, on the other hand, the GDPR is applicable when dealing with cases of the development of Artificial Intelligence where personal data and its use is destined to reach a decision about individual subjects[14].

This legislative instrument bases itself on data processing, which can be, in general lines, any operation or set of operations performed on personal data, whether by automated means or not, such as collection, recording, storage, organization, structuring, among others[15]. All of the actions just mentioned may be performed by an Artificial Intelligence device, and that is the approach adopted in the GDPR, through four strong challenges to the development of these innovations: data minimisation, purpose limitation, fairness and discrimination, transparency and right to information[16]. Although these principles are presented as difficult barriers to cross, one must conceive that, in reality, it is possible to use and develop AI technologies while safeguarding fundamental data protection rights. Nowadays, human behaviour is being highly scrutinized at the expense of decisions based on algorithms, which alerts individuals to the urgency of protecting them.

---

[14] Datatilsynet – The Norwegian Data Protection Authority, *"Artificial intelligence and privacy – Report, January 2018"*, p. 15.

[15] Article 4(2) GDPR.

[16] Datatilsynet – The Norwegian Data Protection Authority, *"Artificial intelligence and privacy – Report, January 2018"*, p. 4.

1.1. Data minimisation principle

To sum this principle in very few words, it resonates in the expression *the need to know is distinct from being nice to have*. In this way, data must be limited to what is necessary to the purpose, as it is clearly stated in article 5(1)(c) of the GDPR. This echoes the necessity for the data to be correct, updated and, most importantly, must not be retained for a longer period of time necessary for the purpose that justified the data collection in the first place.

Recital 156 of the GDPR is also of great importance in this matter. It states that the processing of personal data for purposes of public interest, scientific, historical or statistical research must be subject to appropriate safeguards regarding the rights and freedoms of the data subject – which means, not only, but also, that those safeguards ensure that technical and organisational measures must be put in place in order to guarantee the respect for the principle of data minimisation.

This can easily present as a challenge for individual automated decisions, since it is widely understood that the more training data is inputted in the machine, the better will the result be[17]. It is logical that the more data we feed the machines, the more accurate they will be, so their behaviour will be able to mimic our patterns with a shorter margin of error.

But how can we know where to draw a line? When and how do we know that enough is enough?

Regarding the data minimisation principle, we shall begin with a small sample of training data and then study the machine's learning curve to assess whether we need to input more data, and which data[18].

This principle does not limit itself to the regulation of the amount of data (to be) processed. Because we are dealing with the interference in a data subject's fundamental rights[19], the minimisation principle

---

[17] Datatilsynet – The Norwegian Data Protection Authority, *"Artificial intelligence and privacy – Report, January 2018"*, p. 11.

[18] Datatilsynet – The Norwegian Data Protection Authority, *"Artificial intelligence and privacy – Report, January 2018"*, p. 12.

[19] One can note that, according to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU), data protection and privacy are distinct, as processing of

also stipulates the proportionality of data processing[20]. About this question, the available solution reached to this moment relates to the extension to which is possible to identify the data subject. One can recognize that security measures such as encryption, anonymisation[21] and pseudonymisation[22] are very useful to preserve the data subject's identification, besides restricting the amount and nature of information used in the automated decision-making process[23]. These measures are not exhaustive, as other means exist, such as purposefully restricting the categories of data collected from a data bank, even if the data subject is still identifiable.

1.2. Purpose limitation principle

The definition of the purpose for processing personal data may also present as very complex due to the technical challenges inherent to system's development. At the moment data are collected, the underlying purpose must be already determined, also needing to be specific, explicit and legitimate[24].

---

personal data can be carried on without interfering with the subject's privacy. One may also interfere in a data subject's privacy without perform data processing.

[20] Proportionality is one of the key principles of EU law, as it assures that there is not an unnecessary disregard and violent compression of fundamental rights, like personal data rights – https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en. Consulted on 17 October 2019.

[21] The Irish Data Protection Commission defines anonymisation in its *"Guidance Note: Guidance on Anonymisation and Pseudonymisation"*, June 2019, as the processing of data "(...) with the aim of irreversibly preventing the identification of the individual to whom it relates" (p. 2). This document is available on: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf.

[22] *Idem*, defining pseudonymisation as the replacement of "(...) any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified" (p. 3).

[23] Datatilsynet – The Norwegian Data Protection Authority, *"Artificial intelligence and privacy – Report, January 2018"*, p. 18.

[24] Article 5(1)(b) of the GDPR.

Without adding any explanation, it may seem that the act of processing may later reveal itself forbidden if the purpose is changed in any way. One shall say, then, that the processing should stop immediately if it is incompatible with the original purpose.

This would present as a huge challenge to the development of new technologies in general, as many times it is very difficult – or even impossible – to outline a purpose for the collection and for the afterwards processing of data. The algorithms, when working in a black box AI and Machine Learning systems, can be very uncertain in what they can learn from data, thus the purpose can change as the machine is developed[25].

The key here will be to assess the compatibility between the initial purpose and the "new" purpose on a case-by-case basis. To do this assessment, one may analyse: the relationship between purposes for which the personal data have been collected and the purposes for further processing; the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use; the nature of personal data and the impact of the further processing on the data subjects; the measure adopted by the controller[26] to ensure fair processing and to prevent any undue impact on the data subjects[27].

This means that it is possible to use the data beyond the original purpose in which the collection was based, but this usage cannot be unrestricted and out of control. This is of crucial importance especially

---

[25] Datatilsynet – The Norwegian Data Protection Authority, *"Artificial intelligence and privacy – Report, January 2018"*, p. 18.

[26] In this sense, the controller must always be the one designated for this function by the owner of the system where the data in question is processed. Being the one who determines the how, when and what of processing, it must, however, be conceived that this person can use third parties to carry out the tasks required by the data processing.

However, in cases where there is no coincidence between that person and the person who conceives the algorithm, e.g. when the provision of this instrument is made by a third party without the controller mastering the internal operation of the algorithm, the powers and responsibilities arising from the controller's position as guarantor must cover the third party.

[27] Recital 50 of the GDPR.

regarding data subject's rights to access, rectification, erasure, among others[28].

So, in case that the new purpose presents itself in counterbalance with the purpose that allowed the collection of the data, the controller must assess its compatibility[29]. As said by the Article 29 Data Protection Working Party, before the GDPR came into force, "Further processing for a different purpose does not necessarily mean that it is incompatible: compatibility needs to be assessed on a case-by-case basis"[30]. If the purposes come to be incompatible between them[31], the controller may seek new consent to keep processing the data[32], or analyse which legal basis[33] appears to be more suitable. However, if the new purpose, which was not originally projected, reveals compatible with the original the controller may not need a new lawful basis[34].

---

[28] Datatilsynet – The Norwegian Data Protection Authority, *"Artificial intelligence and privacy – Report, January 2018"*, p. 16.

[29] Article 6(4) of the GDPR established legal basis for further processing. If the controller has collected data on the basis of a contract, legal obligation, protection of vital interests of the data subject or performance of a task carried out in the public interest or in the exercise of official authority, the data can then be used for the new purpose if it reveals compatible with the original (https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en. Consulted on 12 February 2020).

[30] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, adopted on 2 April 2013, page 3.

[31] UK's DPA highlights the cases regarding the changing of lawful basis very clearly: "You must determine your lawful basis before starting to process personal data. It's important to get this right first time. If you find at a later date that your chosen basis was actually inappropriate, it will be difficult to simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements." (Information Commissioner's Office, *Lawful Basis for Processing.* Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/. Consulted on 12 February 2020).

[32] Datatilsynet – The Norwegian Data Protection Authority, *"Artificial intelligence and privacy – Report, January 2018"*, p. 17.

[33] Article 6 of the GDPR, articulated with Article 9 if the processing refers to special categories of data.

[34] Information Commissioner's Office, *Lawful basis for processing*, retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-

Differently, failure to comply with the compatibility requirement will lead to an unlawful data processing, which therefore is not permitted[35].

The purpose limitation is especially important for the data subject in case the data subject desires to exercise control over their own personal information. The main objective of this principle relies on the avoidance of ambiguity of data processing, thus the specification of purposes must be understood by the concerned data subjects (as well as others, such as Data Protection Authorities), disregarding different and linguistic backgrounds, as well as any intellectual or special needs. Through this measure, it will be possible to reduce "(...) the risk that the data subjects' expectations will differ from the expectations of the controller. (...)".[36]

The rights of the data subject are the consequence of data protection being a fundamental right, hence the need of the controllers need to be transparent about how the deal with these rights in a concise, easily accessible manner, with clear and plain language.

This is the reason why the GDPR additionally contemplates the right to information[37], right of access[38], right to rectification[39], right to object[40],

---

data-protection-regulation-gdpr/lawful-basis-for-processing/. Consulted on 12 February 2020.

[35] Article 29 Data Protection Working Party (W29), *Opinion 03/2013 on purpose limitation*, adopted on 2 April 2013, pages 36 and 40.

[36] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, adopted on 2 April 2013, page 17.

[37] Established in Articles 13 and 14, it is stated the controller needs to explain to the data subject what data is processed, for which purpose, by whom and with which parties that data are shared.

[38] Article 15 of the GDPR states that all data subjects have the right to access their own data, following authentication of their entity.

[39] GDPR, in its Article 16, establishes that any inaccurate or incomplete data can be rectified by the data subject.

[40] This right is only applicable in case of processing for public or legitimate interest, or direct marketing. Nevertheless, Article 21 states that it can be overridden by the data controller with compelling arguments.

right to erasure[41-42], right to restriction of processing[43] and right do data portability[44].

1.3. Fairness and non-discrimination

As previously mentioned, there is a tendency to forget that, in the basis of the construction and design of a device, there is a human-being, an engineer or developer, or even a whole team. Thus, we can conceive that

---

[41] Article 17 of the GDPR lays out the scenarios in which the data subject has the right to have his-her information erased from a database: when the data is no longer necessary for its underlying purpose, consent for processing is withdrawn, the right for object is exercised and cannot be overridden, the data have been processed unlawfully, a legal obligation to delete the data applies or data have been collected by *information society services* based on consent by a minor.

[42] A clear example of the importance of this principle is seen in Court of Justice of the European Union, *Google Spain v AEPD and Mario Costeja González* – C-131/12, 13 May 2014, even before the GDPR came into force. (Available on http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en). This decision by the Court of Justice of the European Union establishes the responsibility of an Internet search engine operator (in this case, Google) for the data processing of personal information that appears on web pages published by third parties. In 1998, the name of Mario Costeja González appeared in relation to a *La Vanguardia* article that focused the forced sale of properties arising from social security debts. Later, in 2009, Mario González contacted the newspaper, complaining that, whenever his name entered in the Google search engine, it led to these announcements. *La Vanguardia* replied saying that erasing was not appropriate due to a publication of the Spanish Ministry of Labour and Social Affairs. Thus, González contacted Google Spain asking for the announcements to be removed, while simultaneously lodging a complaint with the Spanish DPA, AEPD. In the end, the Court of Justice of the European Union ruled that whenever the data processing is "inadequate, irrelevant or excessive", it may be incompatible with the Directive 95/46/EC (which is the predecessor of the GDPR).

[43] This right, contemplated in Article 18 of the GDPR, allows the data subject to ask to restrict the processing of his/her data, if the data or lawfulness of processing is contested. Thus, if the process is restricted, the data cannot be further processed without consent of the data subject (or for legal defence).

If data are corrected, erased or the processing is restricted, the data controller has the responsibility to inform all recipients of the changes.

[44] Article 20 establishes that data subjects are entitled to take their data from one data controller to the other if processing is based on consent or contract or the data are processed by automated means. This right empowers data subject while ensuring free flow of data.

there can be discrimination intentionally or unintentionally embedded in the algorithms, especially if the training data generates biased results, and this use of personal data is in clear contradiction with the fairness principle[45].

Biases can originate from a variety of elements related to the development of Artificial Intelligence tech: methods (measurement, survey, pre-processing stages), datasets (social bias due to historical bias and/or misrepresentation of some categories), data sources (selection bias), data scientists (confirmation bias)[46].

So, the controller, owner of the technological device or algorithm or license holder of the algorithm owned by an external service provider, must be responsible – and able – for the implementation of measures that avoid reaching biased results. However, this may reveal itself insufficient to comply with the fairness principle. Thus, assessment and investigation by the controller is needed, in order to ensure this principle is respected[47].

1.4. Transparency and right to information

Transparency[48] is the key right of the data subject: it is in this way that it is assured to him/her that the relevant information is received, that they are given an explanation, at the time of the data collection, of what actions will take place and on what lawful basis the processing relies on. In conclusion, controllers must – again, to be able or in position to – inform the data subject about processing details (these cannot be limited to general lines, must also include rules, risks, safeguards and data subjects' rights)[49]. The information must be provided to data

---

[45] Datatilsynet – The Norwegian Data Protection Authority, *"Artificial intelligence and privacy – Report, January 2018"*, p. 16.

[46] Information presented in Professor Alessandro Mantelero's talk "Personal Data Protection and AI – Challenges and Remedies" (available to watch in https://www.youtube.com/watch?v=Jp3LhIG6M1A).

[47] Datatilsynet – The Norwegian Data Protection Authority, *"Artificial intelligence and privacy – Report, January 2018"*, p. 16.

[48] Article 5(1)(a) of the GDPR.

[49] Datatilsynet – The Norwegian Data Protection Authority, *"Artificial intelligence and privacy – Report, January 2018"*, p. 19.

subjects in a plain, clear and accessible form. Article 71 precisely states that the processing shall be "(...) subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision". Therefore, the controller must be able to explain to data subjects the rationale behind the algorithmic decision-making to the data subjects[50].

It is in this sense that the GDPR stipulates the right to information in its articles 13 and 14. From these rules it is possible to conclude that the obligation for the controller to explain, to the data subject, what data is processed, when not collected directly from the data subject, for which purpose(s), by whom and with which parties the data is shared is clearly established.

So, we can clearly understand how this presents as a challenge to algorithm decision-making advances. The more advanced the technology is, the more difficult it tends to be perceived, mostly because of the complexity of processes behind it[51]. It is also problematic in the sense that we may be dealing with Intellectual Property Rights and commercial secrets, like the Recital 61 of the GDPR establishes[52].

Although these challenges are very present and seem difficult to overcome, it is important to underline that these principles clearly regulate automated decisions, as clearly stated in article 22 of the GDPR. This article establishes that "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her". This article, however, in its paragraph 2, presents three exceptions to that prohibition: when the decision is necessary for the performance of a contract between the data subject and data controller; when the decision is authorized by EU or national law to which the data controller is subject, since this legislation establishes

---

[50] W29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* adopted on 3 October 2017, page 14.

[51] *Idem.*

[52] *Idem.*

measures to safeguard the data subject's rights; when the decision is based on the data subject's explicit consent.

However, there are already authors[53] who argue that the right of explanation established in the GDPR does not represent an answer to the problems mentioned above. Nevertheless, they defend that these explanations have positive aspects, such as helping data subjects/users to trust and make a better use of the systems and allowing them to project a draft of how it works[54]. In this sense, Edwards and Veale advocate that attention should be drifted from the data subjects to the intention of building better systems *ab initio*, as well as give powers to the competent agencies to analyse and eventually correct the algorithms bias, accuracy and integrity[55].

2. GDPR's regulation on automated decision-making

The GDPR may shape the development of Artificial Intelligence and Machine Learning in two distinct manners.

On one hand, this legislative instrument is truly focused on the enhancement of data security, as it states strict obligations to controllers and processors[56], knowing that Artificial Intelligence devices require extreme large data sets of varied nature to analyse, and personal data are, most of the time, among these[57].

All data subjects have the right[58] not to have their data processed uniquely by automated means when those involve decisions with specific effects on data subjects. This is the ultimate goal of article 22(1) of the

---

[53] EDWARDS, Lilian; VEALE, Michael, *Slave to the Algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for*, Duke Law & Technology Review, May 2017. Available here: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855.

[54] *Idem*, page 22.

[55] *Idem*, page 23.

[56] OLEKSIUK, Anna, *How to Train an AI with GDPR Limitations – Learn how AI companies can comply with the new European data protection regulation*, Intellias – Intelligent Software Engineering, 2019. Retrieved from https://www.intellias.com/how-to-train-an-ai-with-gdpr-limitations/. Consulted on 26 October 2019.

[57] *Idem*.

[58] This right is not new: it was already established in article 15 of the Directive 95/46/EC.

GDPR. By "solely automated" the legislator meant "(...) a decision-making process that is totally automated and excludes any human influence on the outcome. A process might still be considered solely automated if a human inputs the data to be processed, and then the decision-making is carried out by an automated system"[59].

The interpretation of article 22 must be in line with the fundamental principles of the GDPR, according to which the data subject has control over the use of their personal data[60]. This means that the prohibition established in this article can only be applied in limited circumstances; more precisely, only if the decision based solely on automated processing or profiling has a legal effect on the data subject[61]. Not to disregard, then, the logical requirement of safeguarding measures, namely the right to be informed (articles 13 and 14) and the right to challenge the decision [article 22(3)][62]. Nevertheless, is very difficult to draw a line regarding what decisions should be considered to "significantly affect him or her", although W29 gave some examples, such as decisions that can affect an individual's financial circumstances, employment opportunities or access to health services and education[63].

A process will not be considered solely automated if someone weighs up and interprets the result of an automated decision before applying it to the individual[64]. Essentially, if someone steps in at some point of

---

[59] Information Commissioner's Office, *What does the GDPR say about automated decision-making and profiling?*. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-does-the-gdpr-say-about-automated--decision-making-and-profiling/. Consulted on 13 February 2020.

[60] Article 29 Data Protection Working Party (W29), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, adopted on 3 October 2017 and last revised and adopted on 6 February 2018, page 20.

[61] *Idem*.

[62] *Idem*.

[63] *Idem*, page 22.

[64] Information Commissioner's Office, *What does the GDPR say about automated decision-making and profiling?*. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-does-the-gdpr-say-about-automated--decision-making-and-profiling/. Consulted on 21 October 2019.

data processing, reviewing the decision, the process no longer fits in this definition.

The legislative instrument that is today the centre of data protection regulation, in its article 22, clearly states that it applies to automated individual decision-making and profiling with legal or similarly significant effects on the data subjects, and this type of processing is restricted[65]. Therefore, for this process of decision-making to be lawful, it must be "necessary for the entry into or performance of a contract; authorized by Union or Member state law applicable to the controller; or based on the individual's explicit consent"[66].

So, what one has to conclude after knowing this is that the controller must assess whether the processing activity fits itself in the scope of the mentioned article. If that is the case, the controller must provide all the processing information to data subjects, introducing simpler ways for them to require human intervention to contest any decision that affects them. The controller must perform all checks to assess the system's regular functioning[67].

Data protection, although being, as referred before, a fundamental right that deserves protection under the Charter of Fundamental Rights of the European Union[68], must not be seen as an unremovable obstacle to the use of innovative and data-driven technologies. The principles mentioned above (data minimisation, purpose limitation, fairness and non-discrimination, transparency and right to information) must serve as guidance for controllers regarding the processed personal data[69].

---

[65] Information Commissioner's Office, Rights related to automated decision making including profiling. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to--automated-decision-making-including-profiling/. Consulted on 21 October 2019.

[66] Article 22(2) of the GDPR.

[67] Information Commissioner's Office, Rights related to automated decision making including profiling. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to--automated-decision-making-including-profiling/. Consulted on 21 October 2019.

[68] Thus, it must be balanced against other fundamental rights contemplated in CFREU, such as the freedom of conducting a business (article 16).

[69] *Idem*.

3. What about Data Protection Impact Assessments?

The GDPR clearly states, namely when using new technologies, that controllers must carry out an assessment of impact of the processing regarding protection of personal data[70] before they begin to process data. These are particularly important when the data processing operations represent a menace or "(...) high risks to the rights and freedoms of natural persons. (...)"[71]. We are talking about a process that allows companies and organizations to identify and minimize risks[72], protecting themselves against possible future fines.

Then, it is easy to understand the need of Data Protection Impact Assessments (DPIAs)[73] while facing the development of decision-making tech. These are particularly useful, hence the fact that they tell if there is a high risk for the individuals' rights that cannot be mitigated, thus imposing[74] controllers the consultation with the competent Data Protection Authority.

DPIAs have proved to be extremely useful for controllers regarding the assessment of risks related to data processing, helping them to assure that their activities fall within the scope of Article 22(1), and in case of identifying an exception, to analyse which safeguarding measures must be applied[75].

---

[70] Article 35(1) of the GDPR; Recital 90 of the GDPR.

[71] Article 35(1) of the GDPR.

[72] Information Commissioner's Office, *Data protection impact assessments*. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/. Consulted on 27 October 2019.

[73] Data Protection Impact Assessments are processes designed to help regarding the identification and minimisation of risks related to data protection. In some cases, they appear as mandatory, specially facing scenarios involving high risk processing tasks that may harm data subject's rights. DPIAs are seen as crucial to mitigate these risks, even though it appears to be very difficult to eliminate these obstacles to data processing.

[74] In this particular case, prior consultation with the competent DPA is mandatory, not optional.

[75] Article 29 Data Protection Working Party (W29), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/67*, adopted on 3 October 2017 and last revised and adopted on 6 February 2018, page 20.

DPIAs are the mirror of two key aspects (which are intertwined) brought by the GDPR: accountability and privacy by design. They are part of a risk-based approach mentioned above and must not be taken light-heartedly. They are presented as guidelines for controllers to go into detail about their processing activities, allowing them to exercise control and to demonstrate accountability for their systems[76].

The Information Commissioner's Office (ICO)[77] points out that "(...) DPIAs will force organisations to demonstrate the necessity and proportionality of any AI-related personal data processing; account for any detriment to data subjects that could follow from any bias or inaccuracy in a system; explain the rationale behind any trade-offs; and describe the relationships and the terms of any contracts with other processors or third party providers. DPIAs can also support organisations in thinking about the broader risks of harm to individuals or ethical implications for society at large. (...)[78]".

Although controllers may see DPIAs as a burden, they may reveal useful as mentioned above, as a preventive risk management measure[79]. These processes, through the audit of algorithms and regular reviews of the automated decision-making, allow controllers to assess and determine if there is the risk of any bias or errors and, in case this happens, to develop measures to minimize the potential harm[80].

---

[76] *Idem*.

[77] Information Commissioner's Office is UK's Data Protection Authority, which is an independent body with the goal of endorsing the information rights in the public interest. More information can be found in the following: link: https://ico.org.uk/about-the-ico/what-we-do/. Consulted on 08 February 2020.

[78] Information Commissioner's Office, https://ico.org.uk/about-the-ico/news-and-events/ai-blog-ai-auditing-framework-call-for-input-final-considerations-and-next-steps/. Consulted on 21 May 2020.

[79] *Idem*.

[80] Article 29 Data Protection Working Party (W29), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* adopted on 3 October 2017 and last revised and adopted on 6 February 2018, page 28. The W29 also draws attention to the need for these processes to be used continuously, not only at the design stage.

A DPIA can also be used to inform the data subject about the underlying logic of an automated decision-making process, allowing him or her to oppose the decision and/or to express their point of view[81].

4. How do we proceed?

In light of everything that has been said, the main question that one can come across is how to make new inventions, new algorithmic decision-making devices, compliant and GDPR-friendly? Or, in a clearer way, how can Artificial Intelligence and GDPR co-exist harmoniously?

The W29 has already called for the need of establishing appropriate safeguards, in light of what is already established in Article 22(2)(a), 22(2)(c) and 22(3), in order to assure data subjects' rights, freedoms and legitimate interests[82]. The working party is very clear when defends that human intervention is crucial in this matter, since "(...) any review must be carried out by someone who has the appropriate authority and capability to change the decision. (...)"[83]. Recital 71 is also very important as it establishes that a data subject has the right not to be subject to a decision based solely on automated processing.

The W29 also highlights that there is a need for transparency regarding the processing of data, thus allowing the data subject to challenge the decision[84].

Artificial Intelligence devices are composed by algorithms that combine data (personal or not) inside their system, and then, after analysing and identifying patterns, give an answer to a proposed problem. As these systems are able to be trained in order to perform all kinds of

---

[81] *Idem,* page 30.

[82] *Idem,* page 27.

[83] *Idem.*

[84] *Idem.*

tasks, sometimes they operate as a black box[85], which raises obstacles in understanding how decisions are reached[86].

To be able to gather all the data the devices need, the controller, taking into account the rules established in GDPR, has to be able to assure that he/she has a lawful basis for the processing of that data. But since it is very difficult to fully understand how the data are being processed inside the machine, especially in the cases in which the systems operate as black box, which means that acquiring consent from the data subject, in its true form, may bring difficulties to perform his/her duties in this regard[87]. Controllers may say that, in a system based in black-box algorithms, "(...) only the algorithm itself can explain its decision-making"[88], though this is not valid for AI systems that function differently.

Controllers, for that matter, shall ensure that the technologies that are being developed by them are fully compliant, respecting the established in article 22 GDPR. Otherwise, they are at great risk of having to pay large fines[89], the amount depending on various criteria, namely the

---

[85] Black box is a concept in Machine Learning that defines the situations which not even the developers are able to explain how the system reached a certain conclusion. Not all Artificial Intelligence systems work this way. On other note, there are systems in which is possible to acknowledge its inner components and functions, thus allowing to get the full picture of how the system works – https://en.wikipedia.org/wiki/Black_box. Consulted on 11 February 2020.

[86] REESE, Hope, *Transparent machine learning: How to create 'clear-box' AI*. TechRepublic, 2016. Retrieved from https://www.techrepublic.com/article/transparent-machine--learning-how-to-create-clear-box-ai/?fbclid=IwAR1a1_O7wGMh3SAQP7Fq5dv76KAH7S8YhNf3vVM6Rz7AiX4D7_pLdVql3H0. Consulted on 11 February 2020.

[87] CAKEBREAD, Caroline, Can AI and GDPR Co-Exist? AI says, 'Give me more data!'; GDPR says, 'Slow down buddy!'. EMarketer, 2019. Retrieved from https://www.emarketer.com/content/what-gdpr-means-for-ai. Consulted on 23 October 2019.

[88] *Idem*. It may seem a viable solution for systems that if the decision-making system, which works as a black box, cannot be explained or totally understood, then the principles (data minimisation, purpose limitation, among others) must be enforced in the parts that we can analyse, which are the inputs (the data given) and the outputs (the answers extracted).

[89] OLEKSIUK, Anna, How to Train an AI with GDPR Limitations – Learn how AI companies can comply with the new European data protection regulation. Intellias – Intelligent Software Engineering, 2019. Retrieved from https://www.intellias.com/how-to-train-an--ai-with-gdpr-limitations/. Consulted on 23 October 2019.

nature of infringement, which type(s) of data was processed, mitigation measures, among others.

So how can we combine decision-making algorithms (and their need for big datasets) and the protection of the fundamental rights of data subjects?

From the point of view adopted in the present work, the solution may go through one of two paths:

1. the reform of GDPR, allowing it to better keep up with tech advances; or
2. development of GDPR-friendly decision-making algorithms.

The first measure may seem easier and/or more practical, because it is easy to see that European innovations will suffer while competing with nations that are not subjected to rules such as the ones established by the GDPR, like the United States and China[90]. The EU strategy presents itself as very distinct from the American and the Chinese approaches. While the US strategy relies in the development of private sector initiatives and self-regulation[91], the Chinese strategy is mainly designed by a strong coordination between the government and private and public investment in AI technologies[92].

In this sense, GDPR greatly limits the development of decision-making technologies, not only by the imposition of respect for the principles of data minimisation, purpose limitation, fairness, non-discrimination and transparency, but also because it requires giving explanations to data subjects that sometimes, neither the controllers/processor nor developers are able to give. This is easy to understand, as the complexity of solutions increases, the more difficult these can be to explain[93]. In this sense, it is

---

[90] CASTRO, Daniel, CHIVOT, Eline, *Want Europe to have the best AI? Reform the GDPR*. International Association of Privacy Professionals (IAPP), 2019. Retrievved from https://iapp.org/news/a/want-europe-to-have-the-best-ai-reform-the-gdpr/. Checked on 23 October 2019.

[91] For example, Microsoft is a company that has its own AI advisory board, while Google also drafted its own AI principles, which are available here: https://blog.google/technology/ai/ai-principles/. Consulted on 09 February 2020.

[92] European Parliament, *EU guidelines on ethics in artificial intelligence: Context and implementation*, European Union, 2019, page 3.

[93] *Idem*.

not convenient to limit the creation and development of new technologies for the sake of being able to explain to others how the machine and the algorithm work.

As referred before about the risk of being fined, the GDPR can present itself as an instrument that discourages the development of decision--making machines. The "fear" of being fined by DPAs for any violation may lead to the absence of innovations, making the EU less competitive worldwide, as mentioned before[94].

Regarding this, the German DPA alerts AI technologies for the need to "(...) observe fundamental rights in line with democratic and rule-of-law principles", as well to the fact that controllers must adopt organizational and technical approaches to make this possible[95].

The Hambach Declaration sets out the need of regulation regarding AI developments, however not being clear where or how to set said limitations, but knowing that there is the need to respect Ethical Principles[96].

The IAPP (International Association of Privacy Professionals), in the person of Daniel Castro and Eline Chivot, is very clear when it argues that the European policy makers have grounds to perform reforms in the GDPR. In their view, "(...) the EU should reform the GDPR for the algorithmic economy by expanding authorized uses of AI in the public interest, allowing the repurposing of data posing minimal risk, removing penalties for automated decision-making, permitting basic explanations of automated decisions, and making fines proportional to harm"[97].

Never to disregard that according to Article 97 of the GDPR[98], by 25 May 2020, and every 4 years after that date, the European Commission will issue a report on the evaluation and review of this legislative instrument to the European Parliament and to the Council[99].

---

[94] *Idem*.

[95] *Hambach Declaration on Artificial Inteligence – Seven Data Protection Requirements, Resolution adopted at the 97th Conference of the Independent German Federal and State Data Protection Supervisory Authorities*, Hambach Castle, 3 April 2019, pages 27 and 28.

[96] *Idem*, page 30.

[97] *Idem*.

[98] This capacity is generically established by Article 17 (2) of the Treaty of the European Union.

[99] To be able to draft these reports, the Commission has the faculty to ask informations to Member States and supervisory authorities. While exercising the competency to deliver these

On the other hand, if one thinks the solution lies within the design of GDPR-friendly algorithms, there are some suggestions already put in place[100]. Among them, there is one that stands out, which is the use of Generative Adversarial Networks (commonly referred as GANs)[101]. In the present work's perspective, these stand out because it related to the way Artificial Intelligence works.

Although it has not been referred before, "behind" Artificial Intelligence, machine and deep learning are neural networks, which are a system inspired in the operations that the human neurons perform. They are aimed to solve many problems, including signal processing and pattern recognition problems, adapting themselves along by the input of more and new information[102].

In this sense, knowing that this is a system that is embedded within the technology that is being developed, Generative Adversarial Networks can be envisioned as a viable solution because they aim to use a reduced amount of data, by using the training dataset more efficiently[103]. It is composed by two neural networks: the generator and the discriminator. Trying to explain in an accessible way, the discriminator is trained with a smaller dataset, but not so small as to introduce bias. Then, the generative network creates synthetic data, based on a randomized input and it learns as it is able to "fool" the discriminator or not. The discriminator through mechanisms of learning adjusts internal parameters proportionally to the error of the output. Thus, the more successful is the generative network in

---

reports, the Commission shall demonstrate causation between the progress of technologies and the need to review the GDPR.

[100] OLEKSIUK, Anna, How to Train an AI with GDPR Limitations – Learn how AI companies can comply with the new European data protection regulation. Intellias – Intelligent Software Engineering, 2019. Retrieved from https://www.intellias.com/how-to-train-an--ai-with-gdpr-limitations/. Consulted on 26 October 2019.

[101] A generative adversarial network consists of a class of machine learning systems that, when given a training set, learns how to generate new data while using the same statistics as before.

[102] ROUSE, Margaret, *DEFINITION – artificial neural network (ANN),* SearchEnterpriseAI, 2019. Retrieved from https://searchenterpriseai.techtarget.com/definition/neural-network. Consulted on 26 October 2019.

[103] *Idem.*

"fooling" the discriminator network, the greater will be the adjustments and the more the discriminator will learn without the need for real data.

However, GANs, alone, may not be the best solution to the problem that controllers are facing with the development of Artificial Intelligence and Deep and Machine Learning.

Other possible solutions are the Transfer Learning[104] and Explainable AI[105] methods, but, as the one described, face the need of big datasets to be trained.

To build accurate and complete models, one may have to combine several technical methods like these or even develop new ones. None of the current techniques presents itself as a definitive answer for the obstacles and questions raised with data protection in the European framework.

Conclusion

In the present work, there was an attempt to lay out some issues raised by the GDPR regarding the harmony between the development of decision--making algorithms and the protection of individual's personal data.

In light of what was analysed, one can come to the conclusion that there is not one right answer. At least, not yet.

Privacy and data protection rights cannot be ignored in any circumstance by the use of AI systems. Hence, it seems reasonable to argue that the best approach must be the one that combines both the need to reform some of the rules laid out by the GDPR and the development of systems that have embedded in them decision-making algorithms that obey the privacy by design and privacy by default principles.

---

[104] MACMAHAN, Brendan, RAMAGE, Daniel, *Federated Learning: Collaborative Machine Learning without Centralized Learning Data*. Google AI Blog, 2017. Retrieved from https://ai.googleblog.com/2017/04/federated-learning-collaborative.html. Consulted on 26 October 2019.

[105] OLEKSIUK, Anna, How to Train an AI with GDPR Limitations – Learn how AI companies can comply with the new European data protection regulation. Intellias – Intelligent Software Engineering, 2019. Retrieved from https://www.intellias.com/how-to-train-an--ai-with-gdpr-limitations/. Consulted on 26 October 2019.

Knowing that, possibly, it is asking too much, one could not choose a different way, without risking putting a burden either on the European legislator or on the developers alone.

I believe this is a teamwork, converging efforts, as, in the end, the main interest is to give proper protection to individuals who come across the scenario in which their data is collected and processed in ways which are too complex for the average person to understand.

For the time being, while there is not (yet!) any innovative leap in the AI and deep and machine learning fields, controllers must, at least, adopt some preventive measures, such as promoting digital literacy and making the algorithmic systems more easily understandable[106], as well as keep performing Data Protection Impact Assessments[107] regarding these systems, allowing to be aware of way the processing of data is being done, thus being possible to help prevent the black-box effect. It is not enough, not even by far, but it is the minimum that must be done to assess if the processing respects individuals' rights, or, if it is not the case, to give a warning sign for the need of performing corrections.

In the respect for fairness and accuracy, knowingly the data protection issues brought by decision-making algorithms, for the author there is not a singular right answer, but, instead, a series of plural efforts, both from the technological and legal fields, assuring data protection rights are respected.

---

[106] This was already recommended before the GDPR came into force, in 2017, by the CNIL (French DPA). Information available here: https://www.cnil.fr/en/how-can-humans-keep--upper-hand-report-ethical-matters-raised-algorithms-and-artificial-intelligence. Consulted in 11 February 2020.

[107] As mentioned above, according to Recital 90 and Article 35 of the GDPR, DPIAs are useful tools to use in any processing activities, although they are mandatory when the processing is likely to result in a high risk to data subjects' fundamental rights. An algorithmic decision-making process is very likely to result in a high risk regarding a subject's rights and freedoms.

O conteúdo do direito fundamental à proteção de dados à luz do novo Regulamento Geral de Proteção de Dados: em especial, a problemática do controlo das decisões automatizadas

Francisca Cardoso Resende Gomes[*]

Resumo: Graças a uma evolução tecnológica galopante, vivemos num mundo computacional omnipresente potenciador de fenómenos analíticos de tratamento e processamento de dados assentes na utilização de algoritmos, como o *Big Data* e o *data mining*. O seu funcionamento permite a criação de nova informação respeitante ao perfil dos cidadãos, caracterizada por se traduzir em inferências de valor altamente imprevísivel e com uma taxa relativamente baixa de verificabilidade, num contributo para a perda de controlo de que os cidadãos atualmente padecem sobre a sua identidade e a forma como são percecionados pelos outros. Como iremos demonstrar ao longo deste artigo, o atual direito fundamental à proteção de dados emerge como um mecanismo com potencialidade para assegurar uma proteção compreensiva a nível constitucional. Impõe-se, todavia, uma reconfiguração deste direito fundamental, no sentido de enquadrar, do ponto de vista interpretativo, uma nova manifestação de tutela subjetiva, apelidada de direito a inferências razoáveis.

Palavras-chave: *direito fundamental à proteção de dados, Big Data, inferências, decisões automatizadas, direito a inferências razoáveis.*

Abstract: Due to a rampant technological evolution, we live in a ubiquitous computational world that promotes analytical phenomena of data processing based on the use of algorithms, such as Big Data and data mining. Its operation allows for the creation of new information regarding the citizens' profile, characterised by being translated into

[*] Licenciada em Direito pela Faculdade de Direito da Universidade de Lisboa (FDUL). Frequenta o *LL.M. in Commercial and Corporate Law* na *Queen Mary University of London*, onde realizou o módulo de *European Data Protection Law*. Este *paper* foi originalmente concebido como um trabalho para avaliação final à cadeira de Direitos Fundamentais sob a regência do Professor Doutor Jorge Reis Novais e orientação do Mestre Tiago Fidalgo de Freitas, a quem se agradece pelos profícuos contributos prestados.

inferences of highly unpredictable value and with a relatively low rate of verifiability, which contributes to the loss of control that citizens currently suffer over their identity and how they are perceived by others. As we will demonstrate throughout this article, the current fundamental right to data protection emerges as a mechanism with the potential to ensure a comprehensive protection at constitutional level. However, it is necessary to reconfigure this fundamental right, in order to frame, from an interpretative point of view, a new manifestation of subjective protection, known as right to reasonable inferences.

Keywords: *fundamental right to data protection, Big Data, inferences, automated decisions, right to reasonable inferences.*

Introdução

Ao consagrar o art. 35.º, a Constituição da República Portuguesa (doravante "CRP") apresentou-se como pioneira na proteção constitucional dos cidadãos perante o tratamento de dados pessoais informatizados, procedendo ao reconhecimento e garantia daquilo que a doutrina portuguesa, por inspiração germânica, veio a designar de "direito à autodeterminação informacional ou informativa"[1].

O direito à proteção de dados não foi, porém, criado num universo cibernético como o de hoje, que comporta a vivência em rede, a socialização eletrónica e a proliferação informativa em redes abertas, tendo-se assistido recentemente a uma modificação da realidade constitucional propiciada pelas novas tecnologias de informação e comunicação.

Mudou, desde logo, a envolvente em que os dados pessoais são recolhidos, processados e utilizados. Fruto de uma galopante evolução

---

[1] Entre outros, CALVÃO, Filipa Urbano, "O direito fundamental à proteção dos dados pessoais e a privacidade 40 anos depois", in *Jornadas nos quarenta anos da Constituição da República Portuguesa*, Almedina, 2017, p. 85; CANOTILHO, José Gomes e MOREIRA, Vital, *Constituição da República Portuguesa – Anotada*, Vol. I, 4.ª ed. revista, Coimbra Editora, 2007, p. 551; CASTRO, Catarina Sarmento e, «40 anos de "Utilização da Informática": O artigo 35.º da Constituição da República Portuguesa», *e-Pública*, vol. 3, n.º 3, 2016, p. 84-99. Disponível em: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S2183-184X2016000300004&lng=pt&nrm=iso. Acedido a: 12.10.2019; FARIA, Paula Ribeiro de, "Anotação ao Artigo 35.º da Constituição", in MIRANDA, Jorge e MEDEIROS, Rui (orgs.), *Constituição da República Portuguesa Anotada,* Tomo I, 2.ª edição, Coimbra Editora, 2010, p. 785.

tecnológica, assistiu-se ao aparecimento de instrumentos de tratamento da informação pessoal distintos dos tradicionais ficheiros eletrónicos, com destaque para as redes sociais, os sistemas de vigilância e, mais recentemente, a Internet das Coisas (fenómeno também conhecido como IoT). Tornam-se percetíveis os desafios colocados a este direito fundamental face à consideração de que, hoje, a recolha, transmissão e conservação de informação é realizada através de dispositivos eletrónicos incorporados em objetos do quotidiano, como os relógios, os automóveis, os eletrodomésticos e as televisões[2].

É graças a este mundo computacional omnipresente que se assiste à acumulação de um volume crescente e diversificado de informação, instantaneamente recolhida e partilhada, que surge como potenciadora de fenómenos como o *Big Data* e o *data mining*. Trata-se da criação de nova informação, consubstanciada em juízos de probabilidades, inferências e previsões respeitantes ao perfil e padrão de comportamento dos cidadãos, como resultado da utilização de algoritmos no relacionamento e análise dos dados pessoais recolhidos nestes novos contextos tecnológicos. A título exemplificativo, pense-se na capacidade demonstrada pelo Facebook para inferir a orientação sexual, a raça e as convicções políticas dos seus utilizadores[3]. Daqui resultam inferências assentes numa taxa relativamente baixa de verificabilidade, porque revestidas de um valor preditivo e contraintuitivo, a que acresce o seu caráter imprevisível igualmente contribuidor para a emergência das preocupações aqui tratadas relativas ao controlo e responsabilização algorítmica.

A urgência da abordagem teórico-prática desta temática é salientada pela consideração de que esta nova existência cibernética tem como pano de fundo uma mudança dos interesses públicos e privados, traduzida na afirmação de objetivos de eficiência na gestão das empresas e dos organismos públicos. Este ambiente promotor do recurso à inteligência

---

[2] Sobre esta temática, veja-se ANTUNES, Luís Filipe, "A privacidade no mundo conectado da Internet das Coisas", *Fórum de Proteção de Dados*, n.º 2, 2016, pp. 52-58. Disponível em: https://www.cnpd.pt/bin/revistaforum/forum2016_2/files/assets/basic-html/page-I.html#. Acedido a: 12.10.2019.

[3] Veja-se, a este propósito, CABANÃS, José González, CUEVAS, Ángel e CUEVAS, Rúben, "Facebook Use of Sensitive Data for Advertising in Europe", *CoRR*, 2018. Disponível em: http://arxiv.org/abs/1802.05030. Acedido a: 11.10.2019.

artificial e aos fenómenos analíticos descritos anteriormente não constitui ficção científica em Portugal, atento o recente investimento na sua implementação em vários setores da Administração Pública[4].

Neste seguimento, este artigo pretende refletir sobre a questão de saber se o conteúdo do direito à proteção de dados não deverá ser alvo de uma atualização no plano constitucional considerando as especificidades traduzidas pelas decisões automatizadas, pois como Tene/Polonetsky referem "In a big data world, what calls for scrutiny is often not the accuracy of the raw data but rather the accuracy of the inferences drawn from the data"[5].

1. Da jusfundamentalidade do direito à proteção de dados

Desde o seu texto originário, aprovado em 1976, que a CRP integra um preceito com a epígrafe "Utilização da informática", tendo sido, assim, pioneira na consagração constitucional de direitos que especificamente protegem os dados pessoais dos cidadãos em relação ao uso das novas tecnologias[6]. Ao consagrar o art. 35.º, a CRP veio conceder expressa autonomia constitucional a um direito do indivíduo à autodeterminação informativa, distinguindo-o da tutela constitucional concedida à reserva da intimidade da vida privada e familiar protegida no âmbito do art. 26.º

---

[4] cfr. Iniciativa Nacional Competências Digitais (INCoDe.2030), *AI Portugal 2030 – An innovation and growth strategy to foster Artificial Intelligence in Portugal in the European context*, 2019. Disponível em https://www.incode2030.gov.pt/sites/default/files/draft_ai_portugal_2030v_18mar2019.pdf. Acedido a: 14.10.19.

[5] TENE, Omer e POLONETSKY, Jules, "Big Data for All: Privacy and User Control in the Age of Analytics", Northwestern Journal of Technology and Intellectual Property, Vol. XI, n.º 5, 2013, p. 270. Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1/. Acedido a: 11.10.2019.

[6] Neste sentido, LOPES, Joaquim Seabra, "O artigo 35.º da Constituição: da génese à atualidade e ao futuro previsível", *Fórum de Proteção de Dados*, n.º 2, 2016, pp. 15-49. Disponível em: https://www.cnpd.pt/bin/revistaforum/forum2016_2/files/assets/basic-html/page-I.html#. Acedido a: 9.05.2020. Porém, o Autor não deixa de referir que, embora o art. 35.º tenha sido introduzido na Constituição originária de 1976, o seu conteúdo atual resulta, em grande medida, da quarta revisão constitucional, ocorrida em 1997, e que visou compatibilizar o dispositivo com o que se preceituava na Diretiva n.º 95/46/CE.

da CRP, e à autodeterminação comunicativa protegida no contexto do art. 34.º da CRP.

Esta autonomia dogmática é ostensivamente tratada pelo Tribunal Constitucional nos Acórdãos n.º 213/2008 e n.º 403/2015, nos quais nos dá conta, em primeiro lugar, da capacidade da CRP para antecipar a imprescindibilidade de uma dicotomia protecional entre reserva da intimidade da vida privada e proteção de dados pessoais, ao promover uma proteção diferenciada, que apenas mais tarde viria a ser reconhecida pela Carta dos Direitos Fundamentais da União Europeia sob a égide dos arts. 7.º e 8.º, reiterando que "... esta proibição [do n.º 4 do art. 35.º] não impede o acesso apenas a dados íntimos de uma pessoa, mas a todos os dados a ela relativos, mesmo que em nada afetem a sua privacidade."[7]; e, em segundo lugar, da distinção entre autodeterminação comunicativa e autodeterminação informativa, afirmando que "O objeto de proteção do direito à autodeterminação comunicativa reporta-se a comunicações individuais efetivamente realizadas ou tentadas e só essas é que estão cobertas pelo sigilo de comunicações. Naquele outro direito [direito à proteção de dados] protege-se as informações pessoais recolhidas e tratadas por entidades públicas e privadas, cuja forma de tratamento e divulgação pode propiciar ofensas à privacidade das pessoas a que digam respeito."[8].

O direito à proteção de dados é composto pelo conjunto de direitos aos quais é reconhecida expressa dignidade constitucional nos demais números do art. 35.º da CRP, entre eles o direito de acesso aos tratamentos de dados pessoais para conhecimento dos dados que lhe pertencem, o direito à retificação dos dados, o direito à atualização dos dados, o direito a conhecer a finalidade dos tratamentos de dados (n.º 1), assim como o direito ao não tratamento de dados cujo processamento se possa revelar especialmente sensível e o direito à não divulgação de dados objeto de tratamento no sentido de proibição do acesso de dados por terceiros (n.º 3).

Neste seguimento, o conteúdo essencial do moderno direito à proteção de dados demonstra tratar-se de um direito fundamental com uma

---

[7] Acórdão do Tribunal Constitucional n.º 213/2008, *Diário da República* n.º 86/2008, Série II de 2008-05-05, p. 19994.

[8] Acórdão do Tribunal Constitucional n.º 403/2015, *Diário da República* n.º 182/2015, Série I de 2015-09-17, pp. 8254-8255. Esta distinção foi reiterada pelo Acórdão do Tribunal Constitucional n.º 464/2019, in *Diário da República* n.º 202/2019, Série I de 2019-10-21, p. 34.

dupla dimensão, positiva e negativa[9]. De facto, a sua natureza de direito, liberdade e garantia aponta, desde logo, para o seu caráter defensivo, estando em causa a tutela da reserva sobre factos cujo conhecimento por terceiros deve depender do consentimento do seu titular. Este direito de defesa e de liberdade com um conteúdo negativo (*Abwehrrecht*) fica garantido mediante a proibição de ingerência do Estado relativamente a dados informativos que pertencem ao cidadão, mas encontra-se concomitantemente dependente de uma prestação normativa por parte do Estado, traduzida na imposição legiferante concorrente para a plena realização da autodeterminação da pessoa.

Por outro lado, o mesmo direito reveste-se de uma natureza positiva, assente num feixe de faculdades e poderes de decisão e atuação relativamente aos dados pessoais, que dotam o titular dos dados de instrumentos que lhe permitem dispor e controlar os dados pessoais objeto de tratamento, seja realizado pelo setor público ou pelo setor privado, vinculando, com força económica e social equiparável, tanto entidades públicas como entidades privadas (*Drittwirkung*[10])[11].

Apesar da dignidade constitucional que lhe é atribuída, a proteção de dados exige a intervenção do legislador, cabendo à lei, conforme estabelece a letra do art. 35.º da CRP, o estabelecimento das exceções aos direitos ou condições de tratamento nele fixadas (por exemplo, exceções à proibição ao acesso a dados de terceiros, tal como consta do n.º 2), bem como a definição do conceito de dados pessoais e das condições aplicáveis ao seu tratamento, atento os termos do n.º 4 do preceito.

Desde 25 de maio de 2018, a referência à "lei e nos termos da lei" é primordialmente preenchida pela regulamentação constante do Regulamento (UE) N.º 2016/679, de 27 de abril de 2016 (doravante "RGPD"), ao revogar a anterior "Lei de Proteção de Dados Pessoais" (Lei n.º 67/98, de 26 de outubro), sendo a sua execução assegurada, no contexto da ordem jurídica nacional, pela Lei n.º 58/2019, de 8 de agosto. Enquanto ato de direito

---

[9] Neste sentido, FARIA, Paula Ribeiro de, *ob. cit.*, p. 789, e, jurisprudencialmente, o Acórdão do Tribunal Constitucional n.º 464/2019, *ob. cit.*, p. 35.

[10] Neste sentido, FARIA, Paula Ribeiro de, *ob. cit.*, p. 790.

[11] Para uma sistematização das faculdades e poderes de natureza positiva, veja-se o Acórdão do Tribunal Constitucional n.º 355/97, *Diário da República* n.º 131/1997, Série I-A de 1997-06-07, p. 2808.

derivado da UE de aplicabilidade direta nas ordens jurídicas nacionais dos Estados-Membros[12], o RGPD providencia, à partida, toda a regulamentação dos mecanismos através dos quais se torna possível o exercício da autodeterminação informacional constitucionalmente consagrada, ao cumprir o dever de ação legislativa constante do art. 35.º da CRP[13].

A jusfundamentalidade do direito da proteção de dados é, pois, caracterizada não só pelas faculdades constantes das normas consagradas na CRP no âmbito do art. 35.º, mas igualmente pelas faculdades constantes da medida legislativa que torna plenamente exequível as garantias aí presentes, ou seja, as faculdades constantes do RGPD. Consequentemente, importa questionar se a disciplina legislativa existente é apta para a proteção dos sujeitos face ao processamento de dados por via algorítmica.

Atendendo aos contornos do presente artigo, cumpre ainda referir que estes direitos não são absolutos, no sentido de que poderão sofrer limitações de conteúdo em determinadas situações e sob determinados pressupostos, face à relação de tensão existente com outros direitos fundamentais, tais como a liberdade de iniciativa privada[14], através de leis restritivas de direitos, liberdades e garantias. Nesta sequência, a operatividade de todo este feixe de direitos faz-se com a orientação de certos princípios que têm vindo a ser elencados pela doutrina[15] e operacionalizados pela jurisprudência constitucional e europeia, com destaque para os princípios da transparência, da especificação das finalidades, da fidelidade e de limitação da utilização.

---

[12] V. o 2.º parágrafo do n.º 2 do art. 99.º do RGPD, em junção com o 2.º parágrafo do art. 288.º do Tratado sobre o Funcionamento da União Europeia.

[13] Na medida em que é diretamente aplicável em todos os Estados-Membros, o RGPD apresenta vantagens face à Diretiva 95/46/CE, a qual estava sujeita a medidas de receção no plano do direito interno. Promove-se, assim, "a aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais" (Considerando 10 do RGPD).

[14] Neste sentido, WACHTER, Sandra e MITTELSTADT, Brent, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI", *Columbia Business Law Review*, 2018, p. 5. Disponível em: https://ssrn.com/abstract=3248829. Acedido a: 13.10.2019.

[15] Para um quadro completo dos princípios em causa, v. CANOTILHO, Gomes, e MOREIRA, Vital, *ob. cit.*, p. 552.

A este respeito, cumpre referir a análise operada pelo Tribunal Constitucional no Acórdão n.º 464/2019, que vem clarificar a possibilidade de restrição expressamente prevista no n.º 4 do art. 35.º da CRP, no inciso final "salvo em casos excecionais previstos na lei", face à ausência de indicação no preceito dos seus pressupostos ou finalidades. Segundo o Tribunal Constitucional, "... a restrição terá de observar, para além da reserva de lei em sentido formal consagrada no artigo 165.º, n.º 1, alínea b), da Constituição, os limites impostos pelo artigo 18.º, n.os 2 e 3: proporcionalidade em sentido amplo; reserva de lei em sentido material; proibição de retroatividade; e inviolabilidade do conteúdo essencial."[16].

2. A problemática do controlo das decisões automatizadas

Atenta a exposição sobre o conteúdo essencial do direito fundamental à proteção de dados, encontram-se reunidas as condições para nos pronunciarmos sobre a capacidade deste direito fundamental, tal como se encontra hoje densificado, para se adaptar ao mundo da *Big Data*, considerando, em particular, a tendencialmente crescente tomada de decisões por inteligência artificial com base em algoritmos que funcionam com recurso a uma variabilidade incontrolável de dados, de onde decorre a proliferação de inferências, previsões, assunções relativas aos cidadãos.

Ao ser confrontado com este novo contexto, o Tribunal de Justiça da União Europeia (doravante "TJUE") defendeu que as inferências são parte integrante do sistema algorítmico de tomada de decisão, não consubstanciando dados pessoais passíveis de controlo pelo titular ao abrigo do direito fundamental em causa[17]. Face a este cenário de inaplicabilidade, o Tribunal Constitucional Alemão havia já ensaiado na sua jurisprudência um novo direito fundamental diverso do direito à autodeterminação informativa, denominado "direito fundamental à garantia da confidencialidade e integridade dos sistemas técnico-informacionais" (*Grundrecht*

---

[16] Acórdão do Tribunal Constitucional n.º 464/2019, *ob. cit.*, p. 49.

[17] Acórdão do Tribunal de Justiça (2.ª seção) de 17 de julho de 2014, *YS c. Minister voor Immigratie, Integratie en Asiel* e *Minister voor Immigratie, Integratie en Asiel c. M e S,* processos apensos C-141/12 e C-372/12, ECLI:EU:C:2014:2081, pars.38-48.

auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme)[18]. Considerando que os sistemas técnico-informacionais permitiriam a criação de dados, maioritariamente produzidos autonomamente pelo sistema, sem a participação consciente do utilizador[19], o BVerfG concluiu que existia uma "lacuna de proteção" subsequente à perda do valor normativo do direito à autodeterminação informativa, atento o facto de se tratarem de realidades que dispensam a intervenção humana direta e consciente.

Todavia, cremos que esta visão que toma como objeto de proteção o sistema técnico-informacional em si não é correta, visto que propugna por uma verdadeira "objetivação" dos direitos fundamentais, deslocando a esfera de proteção para um elemento externo ao indivíduo, com a consequente crise da atual noção de "dados pessoais". A criação do direito-garantia, ao ter como objeto de proteção "sistemas", supõe na argumentação do BVerfG uma "desindividualização" do sujeito titular de dados pessoais, falecendo o recurso dogmático à ideia de autodeterminação informacional, desde logo por via de perda do valor dogmático de uma formulação construída sob o prefixo "auto"[20].

---

[18] Acórdão do BVerfG, Julgamento do Primeiro Senado de 27 de fevereiro de 2008 – 1 BvR 370/07 – pars. 1-333. Disponível em http://www.bverfg.de/e/rs20080227_1bvr037007en.html. Acedido a: 13.10.2019. Este novo direito-garantia foi mais recentemente analisado no Acórdão do BVerfG, Julgamento do Primeiro Senado de 20 de abril de 2016 – 1 BvR 966/09 – 1 BvR 1140/09 – pars. 1-360. Disponível em http://www.bverfg.de/e/rs20160420_1bvr096609en.html. Acedido a: 17.01.2019.

[19] A este respeito, impõe-se dar nota, na esteira de ALEXANDRE SOUSA PINHEIRO, que "a sacralização do consentimento constitui uma das ilusões mais correntes na história da proteção de dados e adquire características de puro logro quando aplicado à Internet, nomeadamente às redes sociais" – PINHEIRO, Alexandre Sousa, *Privacy e proteção de dados: a construção dogmática do direito à identidade informacional*, AAFDL Editora, 2015, p. 812.

[20] Neste sentido, LEPSIUS, Oliver, "Das Computer-Grundrecht: Herleitung – Funktion – Überzeugungskraft" in ROGGAN, Fredrik (org.), *Online-Durchsuchungen: Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008*, Berliner Wissenschafts-Verlag, 2008, pp. 22 e 33. Para uma perspetiva diferente, ROβNAGEL, Alexander e SCHNABELL, Cristoph, "Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationtecnhnischer Systeme und sein Einfluss auf das Privatrecht", *Neue Juristische Wochenschrift*, 49, 2008, p. 3535, segundo os quais o novo direito não protege sistemas que, pela sua técnica, impliquem a existência de dados pessoais de uma forma irrelevante para uma área da vida da pessoa afetada.

Ainda assim, a sua análise não se restringe, no que concerne à proteção do indivíduo relativamente à utilização de mecanismos de decisão automatizada e às inferências que resultam da sua operacionalização, ao recurso ao "direito fundamental à garantia da confidencialidade e integridade dos sistemas técnico-informacionais", tendo numa recente decisão de 18 de dezembro de 2018, aplicado o direito fundamental à autodeterminação informativa, mas reconhecendo a necessidade de conceder uma proteção constitucional mais assertiva atento o nível de danosidade que a utilização dos mecanismos referidos pode infligir na esfera de proteção dos indivíduos.[21]

Como se verá de seguida, defendemos, de modo semelhante, a existência de espaço de manobra dentro do atual regime constitucional, partindo, porém, a nossa argumentação da consideração prévia de que as inferências são também elas dados pessoais.

2.1. As inferências como dados pessoais

Como resultado da ratificação do RGPD, a noção de dados pessoais em vigor no ordenamento jurídico português consiste na "informação relativa a uma pessoa singular identificada ou identificável"[22]. Tendo em consideração a definição apresentada, a determinação do estatuto legal dos dados inferidos levanta dificuldades, particularmente por estar em causa processos *M2M – Machine to Machine*[23]. Neste seguimento, impera o

---

[21] Acórdão do BVerfG, Julgamento do Primeiro Senado de 18 de dezembro de 2018 – 1 BvR 142/15 – par. 37. Disponível em http://www.bverfg.de/e/rs20181218_1bvr014215en.html. Acedido a: 03.02.2019. De acordo com o BVerfG, "the data in question can be aligned with data collected from other sources, allowing for diverse possibilities of use and linking. These possibilities of use and linking may yield further information and thus lead to conclusions that may result in the impairment of the constitutionally protected confidentiality interests of the person concerned as well as the subsequent interference with their freedom of conduct. Furthermore, there is particular potential for interference given the amount of data that can be processed by means of electronic data processing, which could definitely not be handled by conventional means. The increased risk associated with such technical possibilities is matched by the corresponding fundamental rights protection."

[22] V. n.º 1 do art. 4.º do RGPD.

[23] De modo semelhante, CORDEIRO, António Barreto Menezes, "Dados pessoais: conceito, extensão e limites", *Revista de Direito Civil*, A. 3, n.º 2, 2018, p. 304.

recurso ao modelo dos três passos formulado pelo Grupo de Trabalho do Artigo 29.º, que identifica três situações alternativas, em que se entende que se está perante informação relativa a pessoas. São elas o conteúdo, a finalidade ou o resultado[24].

É no âmbito deste último passo que se chega à conclusão de que este tipo de informação deve ser classificado como dados pessoais, na medida em que abrange toda a informação que não incida sobre uma pessoa (conteúdo) e que não vise avaliá-la ou influenciá-la (finalidade), mas que, em abstrato, o permita fazer (resultado). Consequentemente, ainda que se trate de informação não diretamente legível dos dados recolhidos, é dela inferida, apresentando potencial para impactar uma pessoa identificada ou identificável.

Neste sentido se pronunciou recentemente o Tribunal Constitucional, ao reiterar que "Não obstante aqueles dados [dados de tráfego que não envolvem comunicação intersubjetiva] não se reportarem a concretas e efetivas comunicações realizadas ou tentadas entre pessoas, mas apenas entre pessoas e máquinas ou até mesmo entre máquinas (*machine-to--machine communications*) proporcionadas por «agentes de software», a verdade é que podem assentar nos mesmos dados de base dos segundos e, tal como estes, possibilitar a monitorização, vigilância e controlo de movimentos de pessoas, assim como a construção de perfis de utilizadores que comportam riscos evidentes de perda de privacidade."[25]. Esta conceção pode ser ainda complementada pelo Parecer da Comissão Nacional de Proteção de Dados (daqui em diante, CNPD) n.º 38/2017, que refere que, nos dias de hoje, ocorrem comunicações mesmo quando o utilizador do equipamento de comunicação não o aciona direta e intencionalmente, como sucede no caso das atualizações efetuadas pelas aplicações de correio eletrónico ou outro tipo de mensagens, o que significa que a geração e troca de dados são praticamente constantes e ocorrem mesmo quando os indivíduos utilizadores dos equipamentos nada fazem.[26]

---

[24] Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, WP 136, 20 de junho de 2007, p.12. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Acedido a: 14.10.2019.

[25] Acórdão do Tribunal Constitucional n.º 464/2019, *ob. cit.*, p. 42.

[26] V. Parecer da CNPD n.º 38/2017, processo n.º 8243/2017, pp. 7-10.

O facto de as inferências consistirem em assunções com elevado caráter subjetivo e não-verificável, que partem de dados já existentes sobre o titular de dados, não prejudica a classificação anteriormente operada, na medida em que a mesma não está dependente de se tratar de informação exata ou dada como provada[27]. Se assim fosse, estar-se-ia a prejudicar o objetivo último de proteção dos titulares de dados[28].

Tratando-se, portanto, de dados pessoais, as inferências, previsões e assunções beneficiam da proteção que a eles é disponibilizada no plano constitucional. Todavia, cumpre indagar se a regulamentação em vigor, ainda que recentemente alterada, surge preparada para responder aos desafios levantados, prevendo mecanismos aptos e eficientes para a proteção dos titulares de dados.

2.2. Suficiência das pretensões jurídico-subjetivas existentes?

Ao confrontar a regulamentação existente no plano constitucional, propendemos para a conclusão de que as pretensões jurídico-subjetivas expressamente consagradas são insuficientes para uma eficaz proteção do titular dos dados contra o atual contexto tecnológico, mas evidenciam um potencial de proteção aproveitável mediante a adoção de uma abordagem compreensiva.

Primeiramente, cumpre assinalar que a atual legislação adota um maior enfoque na fase do processamento referente ao *input*, comparativamente com os instrumentos de proteção e controlo que emergem referentes ao *output*. Isto é, as faculdades apresentadas estão mais direcionadas para a vigilância do modo como os dados pessoais são recolhidos e tratados, sendo relativamente incipiente a regulamentação existente quanto ao controlo das decisões alcançadas mediante a sua utilização, sobretudo tendo em consideração que as mesmas dão origem ou partem, frequentemente, de

---

[27] Article 29 Data Protection Working Party, *ob. cit.*, p. 6. No mesmo sentido, KLABUNDE, Achim, "DS-GVO Art. 4 Begriffsbestimmungen", in EHMANN, Eugen e SELMAYR, Martin (eds.), *Datenschutz-Grundverordnung*, 1.ª edição, CHBeck, 2017, pp. 7-8.

[28] Neste sentido também se pronunciou o Tribunal Constitucional – v. Acórdão do Tribunal Constitucional n.º 213/2008, in *Diário da República* n.º 86/2008, Série II de 2008-05-05, p. 19994.

inferências e assunções promovidas pelo recurso a fenómenos analíticos que se baseiam em dados não diretamente providenciados pelos sujeitos, mas que a eles dizem respeito.

Observando a legislação europeia sobre esta matéria, denota-se uma tentativa de melhor acautelamento desta segunda fase de tratamento de dados, consagrando-se aquilo a que doutrina vem designando como direito à explicação, que surge associado ao direito a contestar enunciado no 3.º parágrafo do art. 22.º do RGPD[29]. Importa, todavia, ter em consideração o cariz limitado desta nova pretensão jurídico-subjetiva, que advém da aplicação restritiva que tem vindo a ser promovida pelo TJUE. Segundo este órgão jurisdicional, são excluídas do seu escopo as situações em que se pretenda contestar o raciocínio e os parâmetros utilizados aquando da tomada de decisão, afirmando o TJUE que o conteúdo essencial deste direito fundamental não inclui a análise da precisão e correção do processo de tomada de decisão[30]. Afasta-se, assim, a possibilidade de o titular de dados pessoais ter acesso e, por sua vez, contestar o raciocínio analítico por detrás da tomada de decisão[31].

Concomitantemente, é importante deixar claro que são vários os obstáculos que este tipo de pretensão enfrenta na prática. Desde logo, importa recordar que, atualmente, estão em causa maioritariamente decisões assentes em sistemas de *machine learning*, cujo processo analítico é difícil de traduzir para linguagem percetível e inteligível pelos sujeitos, com a agravante de que esses processos estão em constante alteração em razão da aprendizagem que os caracteriza e distingue face aos sistemas algorítmicos tradicionais[32].

---

[29] Para uma visão exaustiva das posições doutrinárias existentes sobre esta temática, v. CALDAS, Gabriela, "O direito à explicação no Regulamento Geral sobre a Proteção de Dados", *Anuário do Direito da Proteção de Dados Pessoais*, 2019, pp. 40-45. Disponível em http://protecaodedadosue.cedis.fd.unl.pt/. Acedido a: 26.10.2019.

[30] Acórdão do Tribunal de Justiça, processos apensos C-141/12 e C-372/12, *YS, M e S c. Minister voor Immigratie, Integratie en Asiel, ob. cit.*, pars. 39-47.

[31] *Idem*, par. 45, e Acórdão do Tribunal de Justiça (3.ª seção) de 20 de dezembro de 2017, *Peter Nowak c. Data Protection Commissioner,* processo C-434/16, ECLI:EU:C:2017:994, pars. 51-54.

[32] Neste sentido, ANALIDE, Cesar e REBELO, Diogo Morgado, "Inteligência Artificial na era *data-driven*: a lógica *fuzzy* das aproximações *soft computing* e a proibição de sujeição a

Finalmente, não se pode deixar de relembrar que o desvendar dos parâmetros em que se alicerça o funcionamento dos autómatos, doutrinariamente conhecido como o dilema da abertura das *black boxes*[33], levanta um problema de confronto com outros interesses constitucionalmente protegidos, podendo pôr em causa a segurança, o interesse económico e comercial das empresas multimédia, os direitos de propriedade intelectual detidos pelas entidades públicas e privadas, afrontando a liberdade de iniciativa privada constitucionalmente consagrada.

Considerações finais: solução preconizada

Chegados a este ponto, reiteramos que a procura por um melhor enquadramento constitucional das novas realidades tecnológicas não passa pela consagração de um novo direito fundamental, impondo-se, sim, a reconfiguração do direito à proteção de dados, no sentido de enquadrar constitucionalmente novas manifestações de tutela subjetiva que se revelam necessárias, o que se traduz, neste âmbito das decisões automatizadas propiciadoras da proliferação de inferências de "alto risco", na implementação de uma proteção compreensiva, *ex-ante* e *ex-post*[34], enquadrada pelo princípio da limitação da utilização à finalidade.

A primeira componente de proteção, enquadrada na dimensão negativa deste direito, exige uma justificação por parte do criador e/ou utilizador dos dados pessoais inferidos relativamente à necessidade do recurso a esse tipo de dados como base do processamento automatizado de decisões, impondo-se, igualmente, a demonstração de que os dados e os métodos analíticos usados para a criação de inferências são adequados

---

decisões tomadas exclusivamente com base na exploração e prospeção de dados pessoais", *Fórum de Proteção de Dados*, n.º 6, 2019, p. 87.

[33] Trata-se de um conceito decorrente da ciência da computação utilizado para referir sistemas de que se conhece somente os dados de entrada e de saída, sem possibilidade de acesso ao seu funcionamento interno. Ao invés, quando são verosímeis ou inteligíveis os detalhes da programação de um sistema de aprendizagem, geralmente associado a aproximações de *hard computing*, dir-se-á ser *white box* a lógica que funcionaliza a extração de conclusões inferidas. – v. ANALIDE, Cesar e REBELO, Diogo Morgado, *ob. cit.*, p. 87.

[34] Igualmente, WACHTER, Sandra e MITTELSTADT, Brent, *ob. cit.*, pp. 4-5.

e estatisticamente fiáveis[35]. Neste seguimento, o titular tem direito a ser informado sobre a criação e utilização de assunções derivadas de dados pessoais a si respeitantes, cabendo ao responsável pelo tratamento de dados demonstrar a finalidade a que se destinam. Deve, por conseguinte, tratar-se de uma finalidade constitucionalmente legítima, impondo-se o recurso a um teste de proporcionalidade, no sentido de a utilização deste tipo de dados ser idónea e necessária no alcance dos benefícios e utilidade previstos. A estas exigências jurídico-constitucionais acrescem, por sua vez, o controlo da legitimidade, determinabilidade, exatidão, atualidade e limitação temporal da criação ou utilização dos dados inferidos.

Em complemento com a componente *ex-ante*, impõe-se uma segunda componente de proteção, agora *ex-post*, que visa a responsabilização algorítmica, permitindo ao sujeito contestar a decisão alcançada mediante a utilização de inferências imprecisas e irrazoáveis, não com vista a alterar o sentido da decisão tomada, mas a retificar os dados nos quais se baseia, sempre à luz da finalidade para a qual esses dados foram recolhidos.

Inspirados por Sandra Watcher/Brent Mittelstadt[36], propomos, enfim, uma nova pretensão jurídico-subjetiva: direito a inferências razoáveis ("*right to reasonable inferences*").

---

[35] Assim determina o Considerando 71 do RGPD. No mesmo sentido, Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, Wp251rev.01, 6 de fevereiro de 2018, p. 26. Disponível em https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826. Acedido a: 14.10.19.

[36] Cfr. WACHTER, Sandra e MITTELSTADT, Brent, *ob. cit.*, p. 4.

A (possível) limitação legal no prazo de conservação dos dados pessoais dos candidatos a emprego

Patrícia Batista Santos*

Resumo: Com o início de aplicação do RGPD e, posteriormente, da Lei de execução nacional, os prazos de conservação dos dados pessoais continuam, genericamente, sem um limite específico definido. Esta situação permite que sejam as empresas a estabelecer os seus próprios prazos, nem sempre com respeito pelos princípios impostos pelo RGPD.
Este artigo discute a possibilidade e a necessidade do legislador nacional implementar uma limitação específica para a conservação dos dados pessoais dos candidatos a emprego.
Para se compreender a importância desta hipótese serão analisados os vários temas relacionados, não só com as disposições relativas ao RGPD, mas também com o contexto em que se encontra inserido.

***Palavras-chave**: Regulamento Geral de Proteção de Dados; Lei de execução nacional; Prazos de conservação; Processo de recrutamento e seleção; Relações laborais.*

Abstract: With the start of the application of the GDPR and, subsequently, the national enforcement law, the storage period for personal data continue, generally, without having a defined specific limit. This situation allows companies to set their own terms, not always with respect for the principles imposed by the GDPR.
This paper discusses the possibility and necessity for the national legislator to implement a specific limitation for the storage of personal data of job seekers.

---

* Mestre em Direito e Gestão na especialidade de Proteção de Dados Pessoais pela NOVA Direito, onde investigou o tema "A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral". Membro do Observatório da Proteção de Dados Pessoais – Projeto criado no âmbito do CEDIS/FDUNL. Frequentou a 8.ª edição do Curso de Proteção de Dados Pessoais organizado pela Jurisnova. Licenciada em Gestão de Recursos Humanos pelo Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa.

In order to understand the importance of this hypothesis, the several topics related not only to the provisions on the GDPR, but also to the context in which it is inserted will be analyzed.

***Keywords**: General Data Protection Regulation; Recruitment and selection process; National law enforcement; Storage period; Employment relationship.*

Introdução

Ao iniciar o ciclo de vida do contrato de trabalho, mais concretamente, na fase de recrutamento, uma das informações a transmitir aos candidatos é o período de conservação dos dados pessoais ou, se tal não for possível, os critérios necessários para definir esse prazo [alínea a) do n.º 2 do art. 13.º do RGPD].

No entanto, na maioria dos casos, essa informação não é transmitida pelo responsável pelo tratamento e, por sua vez, as empresas implementam prazos que não se adequam ao princípio da limitação da conservação [alínea e) do n.º 1 do art. 5.º do RGPD].

Adicionalmente, no momento em que o candidato exerce o direito de aceder aos seus dados pessoais, não são transmitidas, na íntegra[1], as informações estabelecidas no disposto do n.º 1 do art. 15.º do RGPD[2],

---

[1] Através da realização de um estudo de caso sobre o exercício dos direitos do titular de dados em candidatos a emprego, SANTOS afirmou que o responsável pelo tratamento não transmite o conjunto de informações previstas no n.º 1 do art. 15.º do RGPD apesar de estar previsto na lei e ser uma das suas obrigações (n.º 1 do art. 12.º do RGPD). Ver SANTOS, Patrícia – *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*, Lisboa: FDUNL, 2019, p. 76. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf. Acedido a 18.02.2020.

[2] As informações estabelecidas no disposto n.º 1 do presente artigo remetem para: (i) a finalidade do tratamento dos dados; (ii) as categorias de dados tratados (iii); os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados; (iv) o prazo de conservação dos dados pessoais ou, se possível, os critérios usados para fixar esse prazo; (v) a existência de outros direitos do titular; (vi) o direito a apresentar queixa à autoridade de controlo; (vii) as informações sobre a origem dos dados pessoais quando não são recolhidos junto do titular; e (viii) a existência de decisões automatizadas [alíneas a) à h) do n.º 1 do art. 15.º do RGPD].

sobretudo no que toca ao prazo de conservação e à respetiva finalidade do tratamento.

Estes problemas de implementação do RGPD no seio empresarial, remetem-nos para a seguinte questão:

se o RGPD e a lei portuguesa que o executa, a Lei n.º 58/2019[3], não estabelecem prazos concretos para conservar os dados pessoais, deixando essa opção ao critério das empresas e facilitando a violação do próprio princípio da finalidade do tratamento, não deveria existir legalmente uma limitação para a conservação dos dados pessoais?

Para analisar esta problemática o presente artigo irá incidir sobre: (i) as disposições da legislação europeia e nacional que fazem referência ao tema em análise; (ii) o processo de recrutamento e seleção por ser a partir dele que são recolhidos e tratados um vasto conjunto de dados pessoais associados ao candidato; (iii) a importância da finalidade do tratamento para conservar os dados pessoais; (iv) o período de conservação praticado pelas empresas e, por fim; (v) a discussão relativa à possível fixação, por parte do legislador nacional, de um período de conservação dos dados, de forma a respeitar os princípios impostos pelo RGPD.

É necessário discutir esta problemática, uma vez que os dados pessoais dos candidatos desatualizam com grande facilidade, o que torna importante a existência de uma limitação legal para que as empresas possam definir um prazo específico com o intuito de evitar as situações que ocorrem atualmente.

1. Os prazos de conservação segundo o RGPD e a Lei n.º 58/2019

Segundo a alínea e) do n.º 1 do art. 5.º do RGPD, o princípio da limitação da conservação determina que os dados pessoais são conservados de uma forma que permita a identificação dos titulares de dados apenas durante o período necessário para as finalidades a que se destina o tratamento.

---

[3] Lei n.º 58/2019 de 8 de agosto de 2019, que assegura a execução na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento 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.

Como se vê, que o princípio da limitação da conservação não define um ou mais prazos concretos, antes se encontrando profundamente relacionado com a finalidade do tratamento. Do mesmo modo, o considerando 39 do RGPD, indica igualmente que o prazo de conservação deve ser limitado ao mínimo, conservando-se assim os dados apenas durante o período necessário para a finalidade que estiver em causa, sendo neste sentido que o responsável pelo tratamento deve fixar prazos para o apagamento ou a sua revisão periódica.

Ou seja, o legislador europeu, ao não definir prazos limite concretos para conservar os dados pessoais, encarrega o responsável pelo tratamento de assegurar este princípio fixando os seus próprios prazos.

A Lei n.º 58/2019, que entrou em vigor a 9 de agosto de 2019, apresenta uma disposição relativa aos prazos de conservação dos dados pessoais. O n.º 1 do art. 21.º do referido diploma, prevê que o prazo de conservação dos dados é aquele que estiver fixado por (i) norma legal ou (ii) regulamentar e, na falta desta, (iii) o que se revelar necessário para prossecução da finalidade do tratamento.

Ora, das disposições apresentadas surge um problema. Tanto a Lei de execução nacional como o Regulamento não estipulam um ou mais períodos concretos para conservar os dados pessoais, sendo este apenas limitado pela prossecução da finalidade do tratamento.

Não obstante, a CNPD[4] "tem entendido que os dados de candidatos estarão desatualizados ao fim de um ano a contar da recolha"[5].

---

[4] A CNPD é caracterizada como uma entidade administrativa independente, com personalidade jurídica de direito público e poderes de autoridade. Controla e fiscaliza o cumprimento do RGPD e da Lei de execução nacional, bem como das diversas disposições legais e regulamentares relativas à proteção de dados pessoais, com o objeto de defender os direitos, liberdades e garantias das pessoas singulares relativamente ao tratamento de dados pessoais. Neste sentido, a CNPD é a autoridade de controlo nacional [n.º 1 do art. 63.º da Lei n.º 58/2019; art. 2.º da Lei n.º 43/2004, de 18 de Agosto (Lei de Organização e Funcionamento da Comissão Nacional de Protecção de Dados), alterada pela Lei n.º 55-A/2010, de 31 de Dezembro e pela própria Lei n.º 58/2019].

[5] BAIRRÃO, Isabel, *Os dados dos seus colaboradores respeitam o RGPD?*, cit. INFORH. Disponível em https://inforh.pt/os-dados-dos-seus-colaboradores-respeitam-rgpd/. Acedido a 19.09.2019.

2. A utilização de dados pessoais nos processos de recrutamento e seleção

Quando as empresas necessitam de contratar talentos para fazer face às alterações ocorridas no seio empresarial, podem realizar processos de recrutamento e seleção através de uma das duas modalidades: (i) recrutamento interno – dentro da própria empresa – e; (ii) recrutamento externo – realizado por agências privadas de colocação ou por empresas de trabalho temporário que também desenvolvam atividades de seleção de recursos humanos[6].

Apesar da existência destas duas modalidades, os dados pessoais recolhidos durante este processo têm por objeto o tratamento para efeitos de recrutamento e seleção[7]. Neste sentido, é necessário conhecer, não só o processo de recrutamento e seleção em si, mas também todos os dados pessoais que são tratados neste âmbito.

2.1. O processo de recrutamento e seleção

Em primeiro lugar, recrutamento e seleção são duas práticas da Gestão de Recursos Humanos que, apesar de mencionadas em conjunto (e por vezes confundidas), assumem funções distintas[8].

O recrutamento é composto por "um conjunto de técnicas e procedimentos que visa atrair candidatos potencialmente qualificados e capazes de ocupar cargos e oferecer competências para a organização"[9], enquanto

---

[6] Existem diferenças quanto à responsabilidade do tratamento dos dados pessoais nas duas modalidades de recrutamento. No recrutamento interno, o responsável pelo tratamento é a própria empresa; já no recrutamento externo, o responsável pelo tratamento é a empresa de recrutamento e seleção (Ver DUARTE, Tatiana em comentário ao artigo 88.º do RGPD. PINHEIRO, Alexandre Sousa *et al*. – *Comentário ao Regulamento de Proteção de Dados*. Coimbra: Edições Almedina, 2018, p. 666-667).

[7] É uma situação que ocorre com mais frequência no recrutamento externo, ou seja, por empresas de recrutamento e seleção. Porém, o presente artigo apenas refere este tema de forma generalizada.

[8] A seguinte caraterização de recrutamento e seleção não se encontra, enquanto tal, refletida em diferentes regimes ou enquadramentos jurídicos.

[9] CHIAVENATO, Idalberto – *Planejamento, recrutamento e seleção de pessoal: como agregar talentos à empresa*. 7ª ed. rev. e atual. São Paulo: Manole, 2009, p. 68, cit.

que a seleção remete para a filtragem dos candidatos "mais adequados aos cargos existentes na organização, visando manter ou aumentar a eficiência e o desempenho do pessoal, bem como a eficácia da organização"[10].

Neste sentido, o processo de recrutamento e seleção é composto por quatro etapas: (i) Recrutamento; (ii) Filtragem; (iii) Avaliação e; (iv) Integração[11].

I. Recrutamento

Este é o primeiro contacto entre o candidato e a entidade empregadora. Consiste no método de atrair eventuais candidatos a concorrer a uma vaga que determinada empresa está a oferecer. Os métodos de atração variam entre anúncios (que incluem as plataformas *online*, em especial, o *website* institucional e as redes sociais), instituições de ensino e portais de emprego[12].

A partir da publicação do anúncio, o candidato disponibiliza os seus dados pessoais para este efeito – através do CV –, iniciando assim o processo de recrutamento e seleção.

II. Filtragem

Com o envio do CV por parte dos diferentes candidatos que concorreram à vaga, os recrutadores têm a tarefa de reduzir o número de candidatos. Deste modo, é feita uma triagem dos que apresentam as *soft* e *hard skills* necessárias para desempenhar a função[13].

III. Avaliação

Após a filtragem dos CV's, a etapa seguinte é crucial, pelo facto de restringir, ainda mais, o número de candidatos selecionando apenas os que apresentam as competências exigidas pela empresa.

Assim, os recrutadores realizam um vasto conjunto de avaliações de modo a escolher, entre os restantes candidatos, aquele que mais se

---

[10] *Idem*, p. 106, cit.

[11] BOTELHO, Carlos – *Recrutamento e seleção de recursos humanos*. Lisboa: ISCSP, 2016, p. 1-2.

[12] MATOSINHOS, Hélio Borges – *Práticas de Recrutamento e Seleção em Consultoria de Gestão de Recursos Humanos*. Porto: FEP, 2012, p. 4-6. Disponível em https://repositorio-aberto.up.pt/bitstream/10216/70720/2/25190.pdf. Acedido a 26.10.2019.

[13] BOTELHO, Carlos – *Recrutamento e seleção de recursos humanos*. Lisboa: ISCSP, 2016, p. 2.

adequa à função. Após essa seleção e com base nos resultados obtidos pelo candidato, passamos para a última etapa – a integração[14].

IV. Integração

A partir desta etapa, dá-se a transição do candidato para trabalhador. Ou seja, após a seleção dos recrutadores, com base nos resultados obtidos na etapa anterior do candidato para preencher a vaga, inicia-se o processo de contratação que se conclui com a celebração do contrato entre trabalhador e empregador. Por conseguinte, o trabalhador pode dar início ao exercício das suas funções na empresa.

2.2. Os dados pessoais recolhidos durante o processo de recrutamento e seleção

Ao longo do processo de recrutamento e seleção, é recolhida e tratada uma enorme quantidade de dados pessoais, que variam consoante a etapa em que o candidato se encontra.

O n.º 1 do art. 4.º do RGPD, define de forma bastante ampla os dados pessoais como "informação relativa a uma pessoa singular identificada ou identificável" sendo essa identificação direta ou indireta por meio de um identificador. Ou seja, a partir desta definição, verificamos que todos os dados recolhidos nos processos de recrutamento e seleção correspondem a dados pessoais de candidatos.

Mas, afinal, quais são os dados pessoais utilizados durante este processo?

Num primeiro momento, o dado pessoal mais valorizado pelas empresas é o CV[15], por este apresentar um conjunto de informações inerentes ao candidato – identificação, contactos, histórico profissional e académico, as *soft* e *hard skills* – sendo este o elemento utilizado nas etapas de recrutamento e filtragem.

Por conseguinte, para avaliar o perfil do candidato, é necessário recolher mais dados pessoais, de modo a verificar se a pessoa em questão apresenta

---

[14] *Ibidem.*

[15] O que carateriza o CV como dado pessoal são as informações que este contém sobre o candidato.

o perfil adequado para exercer a função oferecida pela empresa. Neste sentido, através da etapa de avaliação, são recolhidos dados: do formulário de candidatura e entrevista; dos resultados obtidos nas dinâmicas de grupo; na avaliação de competências para o desempenho da função; dos testes psicotécnicos e de outros testes e avaliações que podem ser realizadas durante este processo.

Quando o candidato alcança a última etapa – a integração – e é selecionado para preencher a vaga, são recolhidos, na celebração do contrato, dados pessoais relevantes para a execução do contrato[16]. Por exemplo, o número de identificação fiscal e o número de identificação da segurança social são necessários para realizar o processamento salarial.

3. A relevância da prossecução da finalidade do tratamento para conservar os dados pessoais

Após um breve enquadramento sobre o processo de recrutamento e seleção, verificaremos de seguida como a prossecução da finalidade assume um papel importante para a determinação do prazo de conservação dos dados pessoais neste âmbito.

Com efeito, como determina o n.º 1 do art. 21.º da Lei n.º 58/2019, na falta de norma legal ou regulamentar a conservação dos dados pessoais baseia-se na finalidade do tratamento, aplicando-se o princípio da limitação da finalidade [alínea b) do n.º 1 do art. 5.º do RGPD]. Segundo este princípio, os dados são "recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades"[17].

Neste contexto, os dados pessoais devem ser tratados para efeitos de recrutamento e seleção.

---

[16] Quando é celebrado o contrato de trabalho entre o trabalhador e empregador, os fundamentos de legitimidade para o tratamento dos dados pessoais aplicados consistem na execução do contrato, obrigação jurídica e interesse legítimo [alíneas b), c) e f) do n.º 1 do art. 6.º do RGPD].

[17] Alínea b) do n.º 1 do art. 5.º do RGPD.

Assim, as empresas estabelecem, consoante as suas políticas internas, os prazos de conservação dos dados que vão variando de empresa para empresa. Vejamos a seguinte situação:

> o candidato, ao concorrer a uma vaga, é chamado para uma entrevista em que o recrutador transmite um conjunto de informações relativas ao tratamento dos seus dados pessoais (art. 13.º do RGPD), designadamente o (i) prazo de conservação, a (ii) finalidade do tratamento e o (iii) fundamento de licitude.

Ao analisar cada elemento do leque de informações a transmitir ao candidato, destacamos, em primeiro lugar, o período de conservação[18].

Algumas empresas tendem a estabelecer períodos de retenção até um ano, seguindo o entendimento da CNPD sobre esta matéria[19]. Porém, existem outras que estendem esse prazo chegando, em alguns casos, a quatro anos[20], o que pode originar um problema quanto à exatidão dos dados[21].

Em segundo lugar, relativamente à finalidade do tratamento, o candidato tem o direito de saber qual é a finalidade do tratamento dos seus dados pessoais, constituindo uma obrigação do recrutador transmitir essa informação, sobretudo quando o referido elemento é aquele que, à luz da lei nacional, assegura a conservação dos dados.

---

[18] Segundo PINHEIRO, existe a necessidade de indicar o prazo de conservação dos dados pessoais, porém não é percetível que este constitua uma informação adicional, devendo estar elencado no n.º 1 e não no n.º 2 do presente artigo (PINHEIRO, Alexandre Sousa *et al*. *Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra: Edições Almedina, 2018, p. 349).

[19] BAIRRÃO, Isabel. *Os dados dos seus colaboradores respeitam o RGPD?*. INFORH. Disponível em https://inforh.pt/os-dados-dos-seus-colaboradores-respeitam-rgpd/. Acedido a 19.09.2019.

[20] Esta conclusão é retirada do estudo de caso relativo ao exercício dos direitos do titular de dados, nas situações em que o candidato concorre a uma vaga. Realçando os excessivos prazos de conservação praticados pelas empresas que variam entre um a quatro anos. Ver SANTOS, Patrícia, *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*, Lisboa: FDUNL, 2019, p. 73 – 74. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf. Acedido a 19.02.2020.

[21] O princípio da exatidão estabelece que os dados devem ser exatos e atualizados sempre que necessário, devendo ser adotadas medidas adequadas para que os dados inexatos sejam apagados ou retificados [alínea d) do n.º 1 do art. 5.º do RGPD].

Assim verificamos o quão importante é para o candidato, enquanto titular, ter o conhecimento das informações inerentes ao tratamento dos seus dados, de forma a ter um maior controlo sobre os mesmos.

No entanto, apesar de a Lei de execução indicar que o prazo de conservação é o que se revelar necessário para a prossecução da finalidade – quando não exista um prazo definido legalmente – as empresas estabelecem sempre um período de conservação, inexistindo uma prática uniforme neste âmbito. Parece, contudo, que o legislador atribuiu assim um maior peso a este elemento – ou seja, à finalidade – do que à definição de um prazo limite concreto para os dados serem conservados.

4. O prazo de conservação dos dados pessoais dos candidatos

Num processo de recrutamento e seleção são vários os dados pessoais recolhidos relativos ao candidato – os que constam no CV, os que são recolhidos na entrevista, no formulário de candidatura, nas dinâmicas de grupo, nas avaliações de competências, entre outras avaliações/testes. No entanto, quando o processo termina, os dados recolhidos ao longo do mesmo devem, em princípio, ser eliminados se o candidato não preencher a vaga para a qual concorreu[22].

Acontece que as empresas estipulam prazos de retenção dos dados de modo a que os candidatos possam concorrer novamente caso abra uma vaga similar durante esse período. Por conseguinte, o recrutador deve informar os candidatos sobre o tratamento de dados para este efeito, de modo a que estes, se assim o entenderem, se oponham ao tratamento dos dados pessoais[23].

Nestes casos, o consentimento e as diligências pré-contratuais podem ser o fundamento de licitude para o tratamento dos dados pessoais dos candidatos[24]. Vejamos as duas situações.

---

[22] Ponto 13.2 da Recomendação CM/Rec (2015) 5 do Comité aos Estados-Membros sobre o tratamento de dados pessoais no contexto laboral. Disponível em https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a. Acedido a 30.09.2019.

[23] *Ibidem*.

[24] DUARTE, Tatiana em comentário ao artigo 88.º do RGPD. PINHEIRO, Alexandre Sousa *et al.*, *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Edições Almedina, 2018, p. 671.

As empresas de recrutamento e seleção que tratam dados pessoais ao abrigo do fundamento do consentimento baseiam-se na ideia de que este garante a legitimidade para o tratamento dos dados[25].

Todavia, os processos de recrutamento constituem uma fase pré-contratual, em que as partes avaliam o interesse em contratar a pessoa em questão. Neste sentido, quando um candidato envia o CV para uma empresa, está a requerer que a mesma proceda a diligências pré-contratuais que podem conduzir à celebração de um contrato de trabalho; mas isso não implica que o mesmo seja celebrado[26].

O candidato tem a expectativa de que os seus dados pessoais sejam objeto de tratamento com vista a integrar um processo de recrutamento e seleção que poderá conduzir à celebração do contrato. Deste modo, o candidato está a solicitar diligências pré-contratuais, afastando o consentimento como fundamento de legitimidade para o tratamento dos dados[27].

Findo o processo de recrutamento e seleção, os dados pessoais são eliminados por deixarem de ser necessários para a finalidade que motivou a recolha e o respetivo tratamento. Não obstante, nas situações em que são conservados com o conhecimento do candidato devido à possível abertura de vagas similares, o candidato pode opor-se ao tratamento dos seus dados pessoais, na medida em que não pretende que o seu CV continue armazenado na base de dados[28]. No entanto, nesta situação particular, o fundamento de licitude para o tratamento baseia-se no interesse legítimo (alínea f) do n.º 1 do art. 6.º do RGPD). Uma vez que estão em causa os interesses do titular[29], este pode a qualquer momento, opor-se ao

---

[25] *Ibidem*.

[26] *Ibidem*.

[27] *Ibidem*.

[28] Isto pode dever-se ao facto de o candidato, ao concorrer a várias vagas em empresas diferentes e, no momento em que foi selecionado para preencher uma das vagas, não pretender que as restantes continuem a tratar os seus dados.

[29] Quando o titular exerce o direito de oposição, pede ao responsável pelo tratamento que faça a ponderação entre os interesses de ambos em relação ao tratamento dos dados, de modo a que o titular possa opor-se ao tratamento. Ver SANTOS, Patrícia – *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*, Lisboa: FDUNL, 2019, p. 35. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf. Acedido a 21.02.2020.

tratamento dos dados (n.º 1 do art. 21.º do RGPD). Consequentemente, ao exercer este direito, os dados são eliminados uma vez que não existe outro fundamento que justifique o tratamento.

Com o levantamento desta questão, verifica-se que as empresas nem sempre respeitam a finalidade do tratamento para a qual os dados pessoais foram conservados[30].

O candidato quando tem o conhecimento da finalidade atribuída à conversação dos dados através do recrutador, à partida, quando surgir uma nova vaga para a qual concorreu anteriormente[31], o seu CV vai integrar um novo processo de recrutamento e seleção.

Não obstante, não é isso que sucede em todas as situações em que abrem novas vagas. Ou seja, determinada empresa pode abrir uma vaga mas não informa os candidatos que permitiram a conservação dos dados, criando bases de dados extensas e desatualizadas que irão dificultar o acesso por armazenarem um enorme volume de dados pessoais que, de certo modo, são inúteis para os potenciais candidatos e para as próprias empresas[32].

Deste modo, colocamos a seguinte questão:

se a finalidade atribuída à conservação dos dados acaba por não ser, na maior parte dos casos, respeitada, não deveria existir uma limitação legal para que as empresas conservem os dados durante determinado período, respeitando assim o princípio da limitação da conservação?

5. A limitação legal ao período de conservação dos dados pessoais

Apesar de o RGPD e a Lei n.º 58/2019 fazerem uma breve referência aos prazos de conservação dos dados pessoais, não preveem uma limitação específica quanto ao período em que os mesmos podem ser conservados.

---

[30] *Idem*, p. 58.

[31] Ponto 13.2 da Recomendação CM/Rec (2015) 5 do Comité aos Estados-Membros sobre o tratamento de dados pessoais no contexto laboral. Disponível em https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a. Acedido a 05.12.2019.

[32] SANTOS, Patrícia, *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral,* Lisboa: FDUNL, 2019, p. 58. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf. Acedido a 21.02.2020.

Perante esta situação, quem acaba por tomar a decisão quanto ao limite de retenção dos dados pessoais são as próprias empresas. Porém, um dos problemas apontados ao longo do presente artigo, é o facto de as empresas não seguirem o entendimento da CNPD – os dados pessoais dos candidatos desatualizam ao fim de um ano[33] –, violando o princípio da limitação da conservação.

Com efeito, as empresas praticam longos períodos de conservação e, por vezes, não informam sobre a duração e a finalidade do tratamento dos dados – esta é uma situação que se verifica nas políticas de privacidade disponíveis nos *websites* institucionais e através do direito de acesso aos dados (art. 15.º do RGPD)[34].

Quando falamos de longos períodos de conservação, referimo-nos a intervalos entre um a quatro anos[35]. Como é sabido, o princípio da limitação da conservação apenas admite a conservação por períodos mais longos do que o período necessário para as finalidades para as quais são tratados quando os dados sejam tratados exclusivamente para fins de arquivo de interesse público, investigação cientifica ou histórica ou para fins estatísticos, em conformidade com o n.º 1 do art. 89.º do RGPD [alínea e) do n.º 1 do art. 5.º do RGPD].

Os dados pessoais em causa não correspondem às exceções mencionadas, o que resulta no incumprimento do princípio da limitação da conservação por parte das empresas.

No entanto, as empresas são obrigadas a manter o registo dos processos de recrutamento por um período de cinco anos, por força do n.º 1 do art. 32.º do CT[36]. Com base neste artigo, segundo Duarte, a conservação

---

[33] BAIRRÃO, Isabel, *Os dados dos seus colaboradores respeitam o RGPD?*. INFORH. Disponível em https://inforh.pt/os-dados-dos-seus-colaboradores-respeitam-rgpd/. Acedido a 19.09.2019.

[34] SANTOS, Patrícia, *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*, Lisboa: FDUNL, 2019, p. 73 – 74. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf. Acedido a 21.02.2020.

[35] *Ibidem*.

[36] O presente artigo estabelece que todas as empresas devem manter o registo dos processos de recrutamento efetuados durante cinco anos, devendo constar com desagregação por sexo: os convites para o preenchimento de lugares; os anúncios de oferta de emprego; o número de candidaturas para apreciação curricular; o número de candidatos presentes nas entrevistas de pré-seleção; o número de candidatos a aguardar ingresso; os resultados obtidos nos testes e provas de admissão ou seleção e; os balanços sociais relativos a dados que permitam analisar

dos dados curriculares de um candidato em processo de recrutamento poderá ser alargada por um período máximo de cinco anos, podendo ser considerada como um interesse legítimo da empresa [alínea f) do n.º 1 do art. 6.º do RGPD]. Isto deve-se ao facto de a finalidade da conservação coincidir com a que determina a recolha dos dados, demonstrando que os interesses da empresa podem prevalecer sobre os direitos e liberdades do titular[37].

Todavia, discordamos desta ideia, pelo facto de o período em questão conduzir a bases de dados desatualizadas, fruto do ritmo com que os dados pessoais desatualizam nos dias correntes.

Apesar de prevalecer o interesse da empresa sobre o do titular, esta irá tratar dados desatualizados, onerando os responsáveis pelo tratamento na obrigação de contactar o titular para proceder à retificação dos dados, sempre que ocorra uma revisão periódica.

Por exemplo, se os responsáveis pelo tratamento realizarem revisões periódicas ao fim de doze meses, durante os cinco anos em que os dados pessoais são armazenados na base de dados, o titular durante esse período, será constantemente contactado para proceder à retificação dos dados de modo a que estes sigam o princípio da exatidão. Como verificamos, esta não é a situação ideal, em termos de tempo e alocação de recursos, nem justifica um período de conservação tão extenso.

Com base nas situações descritas pode questionar-se se o legislador nacional não deveria implementar um limite máximo – inferior a cinco anos – para que os dados pessoais dos candidatos fossem conservados, de modo a respeitarem os princípios impostos pelo RGPD?

Através da rápida desatualização que os dados pessoais dos candidatos sofrem por investirem na sua formação, apresentado um *know-how* cada vez mais especializado que as empresas procuram incessantemente para rentabilizar a sua competitividade face às restantes, sugerimos que o

---

a existência de eventual discriminação de pessoas de um dos sexos no acesso a emprego, formação, promoção profissional e condições de trabalho. No entanto, os dados pessoais que concretamente o empregador está obrigado a conservar ao abrigo do presente artigo são os resultados obtidos nos testes e provas de admissão – dados curriculares do candidato.

[37] DUARTE, Tatiana em comentário ao artigo 88.º do RGPD. PINHEIRO, Alexandre Sousa *et al.*, *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Edições Almedina, 2018, p. 670.

legislador nacional defina um limite máximo de seis meses para que os dados pessoais dos candidatos constem da base de dados e, atingindo esse limite, os dados sejam excluídos da mesma.

A redução do prazo de conservação de um ano para seis meses deve-se ao facto de a sociedade estar em constante evolução e o rápido desenvolvimento tecnológico originar a desatualização da informação num curto espaço de tempo. Neste sentido, serão respeitados os princípios estabelecidos pelo RGPD, mais concretamente os princípios da exatidão e limitação da conservação (alíneas d) e e) do n.º 1 do art. 5.º do RGPD).

Através destas questões o legislador nacional deveria atuar de modo a que exista um limite estabelecido legalmente para que as situações como as que foram descritas não se verifiquem. Os dados pessoais são um bem valioso para as empresas e estes devem ser salvaguardados e protegidos tal como determina o art. 8.º da CDFUE e art.º 16.º do TFUE (considerando 1 do RGPD).

Conclusão

O RGPD e a Lei n.º 58/2019 não estabelecem nenhum prazo de conservação específico, apenas mencionam que esse prazo deve ser assegurado através da prossecução da finalidade do tratamento por não existir norma legal ou regulamentar que estipule um limite.

Não obstante, a CNPD tem entendido que os dados pessoais dos candidatos desatualizam ao fim de um ano a contar desde a data da recolha[38].

Entretanto, apesar da maioria das empresas seguir esse período, existem outras que o estendem[39], conduzindo ao incumprimento das normas do RGPD, mais concretamente, ao princípio da limitação da conservação e da exatidão dos dados.

---

[38] BAIRRÃO, Isabel, *Os dados dos seus colaboradores respeitam o RGPD?*. INFORH. Disponível em https://inforh.pt/os-dados-dos-seus-colaboradores-respeitam-rgpd/. Acedido a 19.09. 2019.

[39] SANTOS, Patrícia, *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*, Lisboa: FDUNL, 2019, p. 73 – 74. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf. Acedido a 24.02.2020.

Neste sentido, para compreender como é importante existir uma limitação legal quanto aos prazos de conservação, é necessário conhecer o conjunto de dados pessoais que respeitam ao candidato quando este integra um processo de recrutamento e seleção, e consequentemente, quais são tratados em cada etapa do respetivo processo.

O período de conservação dos dados pessoais é fundamental, no sentido em que o candidato, caso não seja selecionado para preencher a vaga para a qual concorreu, terá a possibilidade de se candidatar novamente quando abrir uma vaga similar, o que se traduz na finalidade do tratamento dos dados pessoais atribuída, isto é, para efeitos de recrutamento e seleção.

Todavia, a finalidade do tratamento em questão, nem sempre é respeitada como objeto para o tratamento dos dados e, para agravar a situação, o período de conservação pode ser longo o que causa dúvidas quanto à exatidão dos dados pessoais, mas também tem impacto na dimensão e atualização das bases de dados.

Apesar de ter uma ligação indireta e constituir um dos problemas resultantes da temática analisada, verifica-se que grande parte das políticas de privacidade das empresas não fazem referência ao período de conservação e à finalidade do tratamento dos dados[40]. O que indica claramente que o princípio da transparência[41] [alínea a) do n.º 1 do art. 5.º do RGPD] não está a ser cumprido pelo facto de não transmitir ao candidato informações relacionadas com o tratamento dos seus dados pessoais.

Perante esta situação, as políticas de privacidade devem ser desenhadas por uma equipa multidisciplinar que, além de ter conhecimentos aprofundados ao nível do direito da proteção de dados pessoais, também conheça o *core business* da empresa. Esta questão é fundamental para demonstrar a transparência exigida pelo RGPD em relação às políticas

---

[40] *Idem*, p. 78.

[41] O princípio da transparência exige que as informações ou comunicações relativas ao tratamento de dados pessoais do titular sejam de fácil acesso e compreensão através de uma linguagem clara e simples, sobretudo, quando estas são fornecidas ao titular sobre a identidade do responsável pelo tratamento e aos fins a que se destinam o tratamento, como, a salvaguarda do seu direito a obter a confirmação e a comunicação dos dados que lhe dizem respeito (considerando 39 do RGPD).

de privacidade, mas também por ser através delas que os prazos de conservação são estabelecidos.

Neste sentido, de forma a evitar que situações desta natureza ocorram, é necessário que o legislador nacional implemente um limite específico quanto ao período de retenção dos dados para finalidades de recrutamento e seleção de forma a que os princípios estabelecidos pelo RGPD sejam respeitados. Tal poderá originar uma restruturação das bases de dados das empresas para que estas apenas armazenem dados pessoais exatos e atualizados para a finalidade a que se destinam, estando assim em conformidade com o RGPD.

Índice Geral

O Anuário da Proteção de Dados é uma revista jurídica de livre acesso, disponível em linha no sítio https://protecaodedadosue.cedis.fd.unl.pt, que pretende divulgar estudos doutrinários sobre o direito da proteção de dados pessoais. O Anuário é editado desde 2018 pelo Observatório da Proteção de Dados Pessoais, um grupo de investigação criado em 2016 no CEDIS – Centro de I & D sobre Direito e Sociedade da Nova School of Law. Aberto a qualquer interessado, o Observatório integra atualmente onze investigadores (três doutorados) oriundos de faculdades de direito (professores e doutorandos), de empresas e do setor público.

Os cinco artigos publicados na edição de 2020 do Anuário resultam de uma chamada lançada em setembro de 2019 no sítio da internet do Observatório da Proteção de Dados Pessoais. Os textos foram depois sujeitos a um processo de blind peer review e posteriormente revistos pelos coordenadores do Anuário.

Jurisnova
Associação da Faculdade de Direito da Universidade Nova de Lisboa

SRS ADVOGADOS

FUTURA