ANUÁRIO
DA PROTEÇÃO DE DADOS
2022

COORDENAÇÃO
FRANCISCO PEREIRA COUTINHO
GRAÇA CANTO MONIZ

CEDIS
CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

ANUÁRIO
DA PROTEÇÃO DE DADOS
2022

ANUÁRIO DA PROTEÇÃO DE DADOS

2022

COORDENAÇÃO
FRANCISCO PEREIRA COUTINHO
GRAÇA CANTO MONIZ

CEDIS
CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ANUÁRIO DA PROTEÇÃO DE DADOS 2022
ANO 5 - 2022

COORDENAÇÃO
Francisco Pereira Coutinho
Graça Canto Moniz

SECRETÁRIO EXECUTIVO E EDITOR
Martim Farinha

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: IMPRESSO
Impressão: 150 exemplares

Setembro, 2022

ISSN 2184-5468

CATALOGAÇÃO NA PUBLICAÇÃO
PEREIRA COUTINHO, Francisco e CANTO MONIZ, Graça
(coord.). Anuário da Proteção de Dados 2020. Lisboa: CEDIS, 2022

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 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 sete artigos publicados na edição de 2022 do Anuário resultam de uma chamada lançada em outubro de 2021 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 João Carrilho sobre o princípio da administração aberta e proteção de dados pessoais, seguindo-se um artigo do Christiano Aguiar que trata o tema dos conflitos entre a proteção de dados pessoais e os deveres de branqueamento de capitais no âmbito do tratamento de dados pelas instituições financeiras. Os algoritmos são novamente abordados no Anuário, pelo Frederico Sequeira, num texto sobre contratação e despedimento de trabalhadores. De seguida, o Joel Alves debruça-se sobre administração eletrónica, eficiência e proteção de dados pessoais. O Diogo Fonseca, a Inês Aires, a Isabel Chowdhury e a Margarida Pereira apresentam uma abordagem prática sobre o regime das transferências de dados pessoais e, por fim, o Sérgio Correia escreve sobre o direito de oposição e a Joana Figueiredo aborda o tema da anonimização no contexto das cidades inteligentes.

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, à Cíntia Pereira de Lima, ao Domingos Farinho, ao Eduardo Magrani, à Helena Tapp Barroso, à Inês Oliveira, ao José Pedro Paiva, ao Luís Neto Galvão, ao Mateus Carvalho, ao Martim Farinha, ao Rui Lanceiro e ao Tiago Melo Cartaxo. Por fim, agradecemos ao Martim Farinha o auxílio prestado na edição do Anuário, bem como a todos os autores que participam nesta edição.

Lisboa, 18 de agosto de 2022

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

Índice Sumário

Compatibilidade do Princípio da Administração Aberta com o Princípio da Proteção de Dados, no contexto do Regulamento Geral de Proteção de Dados

*JOÃO RAFAEL PALMEIRO CARRILHO**

Resumo: Procurámos explorar dois princípios conformadores da atividade administrativa a que o novo Código de Procedimento Administrativo (CPA) veio dar destaque. Começamos pelo princípio da administração aberta, com uma incursão pelo regime constitucional e pela Lei de Acesso à informação administrativa (LADA). Analisámos, depois, o Princípio da Proteção de Dados Pessoais, como ele surge na legislação nacional, nas fontes primárias de Direito da União Europeia e no Regulamento Geral de Proteção de Dados. Por fim, demonstrámos a compatibilidade das condições de licitude de tratamento de dados do regulamento com as condições impostas pela LADA, para o acesso aos documentos nominativos.

***Palavras-chave**: Administração Aberta; Dados Pessoais; LADA; RGPD; Documentos Nominativos*

Abstract: We sought to explore two principles that conform administrative activity that the new Administrative Procedure Code (CPA) has highlighted. We started with the principle of open administration, with an incursion through the constitutional regime and the Law of Access to Administrative Information (LADA). Then, we, analysed the Principle of Personal Data Protection, as it

* Advogado estagiário na PLMJ. Licenciado em Direito pela Nova School of Law. Frequenta o Mestrado em Direito Administrativo na Faculdade de Direito da Escola de Lisboa da Universidade Católica.

appears in the national legislation, in the primary sources of European Union Law, and in General Data Protection Regulation. Finally, we demonstrated the compatibility of the data processing lawfulness conditions of the regulation with the conditions imposed by LADA, for access to named documents.

Keywords: *Open Administration; Personal Data; LADA; RGPD; Nominative Documents*

1. Introdução

No presente trabalho, procurámos estudar, ainda que de forma breve e concisa, a harmonização entre os princípios da administração aberta, consagrado no art. 268º nº 2 da Constituição da República Portuguesa (CRP) e no art. 17º do Código de Procedimento Administrativo (CPA) e o princípio da proteção de dados, com respaldo no art. 35º da CRP e, desde 2015, no art. 18º do CPA. A importância e regularidade do confronto, é patente no número de vezes que a Comissão de Acesso a Documentos Administrativos (CADA) tem vindo a dar parecer sobre a compatibilidade do acesso a documentos administrativos com a proteção de dados pessoais. Assim, pesquisando no motor de busca do *site* da Comissão, surgem cerca de meio milhar de resultados para "dados pessoais".

Neste sentido, a nossa análise dirigiu-se, de seguida, para as condições de acesso a documentos nominativos, tal como definidas pela Lei de Acesso aos Documentos Administrativos (LADA)[1] e para os pressupostos de licitude que o Regulamento de Proteção de Dados Pessoais (RGPD)[2] define para o tratamento de dados pessoais.

Ora, tendo a Lei 58/2019[3], de execução do RGPD, remetido para a LADA, a regulação do acesso a dados pessoais, no âmbito do direito de acesso a arquivos e registos administrativos, a nossa análise terminou com uma tese de conciliação entre os requisitos constantes do Regulamento Europeu e as exigências da LADA para o acesso a documentos nominativos.

1 Lei nº 26/2016, de 22 de agosto.

2 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

3 Lei nº 58/2019, de 08 de agosto.

Para este fim, recorremos, sobretudo à muita doutrina escrita sobre o tema, mas também, a pareceres da CADA e do Comissão Nacional de Proteção de Dados (CNPD) bem como jurisprudência dos tribunais superiores. Em matéria europeia, para além, de alguma doutrina especializada, socorremo-nos dos pareceres do "Article 29 Data Protection Working Party" (WP29)[4] a fim de detalhar as disposições do RGPD e os detalhes da sua aplicação.

2. Princípio da administração aberta

2.1. Da sua previsão constitucional e no CPA

Iniciaremos a nossa análise com uma breve passagem pelo princípio da transparência, seguindo as lições de Sérvulo Correia, segundo o qual os direitos à informação procedimental e o direito de acesso a arquivos e registos da administração (de que nos ocuparemos no presente trabalho), "são, na verdade, duas diferentes concretizações de um mesmo princípio geral de publicidade ou transparência da administração (...)"[5].

O art. 268º da CRP prevê, então, no seu nº 1 e nº 2, direitos de acesso à informação administrativa, dependendo o seu conteúdo e alcance da situação do respectivo titular face à Administração. Assim, com base no estatuto de interessado num procedimento em curso, a Constituição distingue entre:

O direito de acesso à informação procedimental**,** que é reconhecido aos cidadãos "que sejam diretamente interessados*"* num procedimento conducente à formação de uma decisão (constante do nº 1).

O direito de acesso aos arquivos e registos administrativos, na titularidade de todos, independentemente de qualquer procedimento administrativo, previsto no nº 2.

O direito de acesso aos arquivos e registos administrativos foi introduzido pela revisão Constitucional de 1989, inspirado no histórico de transparência documental da administração que vinha sendo desenvolvida nos países

4 Este grupo de trabalho corresponde ao atual Comité Europeu de Proteção de Dados Pessoais (EDPB)

5 Sérvulo, José Manuel Correia; "O Direito à informação e os Direitos de Participação dos Particulares no Procedimento e, em Especial, na Formação da Decisão administrativa"; in Cadernos de Ciência da Legislação, nº 9/10, janeiro-junho, 1994, pág. 135.

escandinavos e que, no termo do século passado, se afirmou em países como França, Espanha e Itália[6].

Não obstante a separação formal, estabelecida pelo legislador constituinte, o Tribunal Constitucional, na prática, tem procedido, nas palavras de Jorge Miranda e Rui Medeiros, a uma interpretação conjunta dos dois preceitos, consagrando "um vasto direito à transparência documental do procedimento"[7].

Adicionalmente, este Tribunal tem-nos considerado, como direitos fundamentais de natureza análoga aos direitos, liberdades e garantias aplicando-lhes o respetivo regime jurídico, com destaque para os art. 17º e 18º da CRP[8]. De resto, a natureza de direito fundamental análogo foi reiterada pelo Acórdão nº 254/99 do Tribunal Constitucional: "O direito de acesso do interessado nunca pode ser menor do que o do cidadão em geral, até porque o interesse público na transparência da atividade administrativa ou numa "administração aberta", como forma de garantia do respeito pelos princípios constitucionais, norteadores dessa atividade, da igualdade, da proporcionalidade, da justiça, da imparcialidade e da boa-fé, só pode ser favorecido pela ação dos diretamente interessados e está na prática dependente dessa ação. (…)"[9].

Assim, como referem, Gomes Canotilho e Vital Moreira, estes direitos constituem "garantias jurídicas perante a administração*"* que dotam os cidadãos de direitos procedimentais e processuais que, não só cumprem a clássica função defensiva perante a administração, como garantem, ainda, "a transparência e a abertura ao funcionamento das administrações exigidas pelo princípio democrático republicano"[10].

Contudo, para o princípio da administração aberta, ganha principal relevância o art. 268 nº 2, depois concretizado pelo art. 17º do CPA e pela

---

6 Miranda, Jorge e Medeiros, Rui; Constituição Portuguesa Anotada; Tomo III; 1ª ed.; Coimbra Editora; 2007; pág. 600.

7 Miranda, Jorge e Medeiros; Rui. Constituição Portuguesa Anotada; Tomo III; 1ª ed.; Coimbra Editora; 2007; pág. 598-599.

8 Miranda, Jorge e Medeiros; Rui. Constituição Portuguesa Anotada; Tomo III; 1ª ed.; Coimbra Editora; 2007; pág. 598.

9 Pinheiro, Alexandre Sousa. "A Proteção de Dados no Novo Código de Procedimento Administrativo", in Comentários ao Novo Código de Procedimento Administrativo; Volume I; AAFDL Editora; 2016; Pág. 335-362; Pág. 353

10 Canotilho, José Joaquim Gomes e Moreira Vital; Constituição Da República Portuguesa Anotada; Tomo II; 4ª Ed.; Coimbra editora; 2010; pag. 820.

LADA[11].

Aqui reside a sua principal garantia, explicitando que os registos e arquivos administrativos são um património coletivo sendo, em regra, de acesso livre e generalizado.

O princípio da administração aberta vem concretizado, ao nível infraconstitucional, no art. 17º do CPA.

Neste dispositivo se estabelece, em primeiro lugar, um direito geral de acesso aos arquivos e registos da Administração, impondo algumas restrições ao mesmo e, num segundo momento, remete-se, como de resto já se retirava do primeiro, para lei extravagante, a regulação das restrições e do regime de acesso aos documentos administrativos. Esta consta, hoje, da Lei 26/2016 de 22 de agosto (LADA).

O artigo em estudo, não é uma inovação do CPA de 2015, estando já presente no art. 65º do CPA de 1991. Contudo, o novo CPA veio atribuir-lhe maior protagonismo, ao consagrar o princípio da administração aberta na Parte I ao invés da sua anterior posição, mais periférica, na Parte III do CPA de 1991. Tornou-se, assim, num princípio conformador de toda a atividade administrativa e não apenas um princípio procedimental[12].

Importa, agora, definir o objeto e âmbito do direito de informação não procedimental conferido pelo art. 268º nº 2. Quando se referiu aos arquivos e registos, o legislador constituinte quis abranger todos os centros ou locais onde se guardam e circulam documentos administrativos[13].

O referido acesso é independente de qualquer procedimento em curso, distinguindo-se, assim, do direito à informação procedimental previsto no art. 82º do CPA, que apenas atribui aos interessados num procedimento em curso, o direito a aceder à informação nele contida.

O art. 17.º do CPA, derivando do art. 268º nº 2 da CRP é diretamente aplicável (art. 17º e 18º n.º 2 da CRP), vinculando as entidades públicas que só podem negar o acesso aos documentos requeridos nos casos constitucional e

11 Acórdão do TCA-SUL de 16-01-2018; P. 1087/17.2BERLRA; disponível em <http://www.dgsi.pt/>

12 Moncada, Luís S. Cabral; Código do Procedimento Administrativo Anotado; 2ª Ed.; Quid Juris; 2017; pág. 124.

13 Miranda, Jorge e Medeiros, Rui; Constituição Portuguesa Anotada; Tomo III; 1ª ed.; Coimbra Editora, 2007, pág. 602.

legalmente previstos.

Quanto aos seus titulares, este direito é concedido a todos, não exigindo que os requerentes do acesso aos arquivos e registos estejam envolvidos num procedimento que lhes diga diretamente respeito[14]. De resto, é, ainda, pacífico que, tal direito, não está reservado a "cidadãos portugueses, no pleno gozo dos seus direitos civis e políticos", pertencendo a qualquer pessoa, sem necessidade, em princípio, de qualquer legitimidade ou justificação[15].

Tal acesso poderá ser feito através de consulta presencial, mas este direito abrange, também, o direito à reprodução de documentos[16].

Não se tratando de um direito absoluto, a própria constituição prevê alguns dos bens fundamentais em nome dos quais este direito pode ser restringido, nomeadamente, "a segurança interna e externa", a integridade de uma "investigação criminal e a intimidade das pessoas". Em adição, o CPA, não só segue a Constituição, como ainda refere o "sigilo fiscal"[17].

Paulo Otero refere que, ainda que numa lógica de maioria de razão, o acesso aos arquivos e registos da Administração, estará vedado quando se refira a documentos que contenham segredos comerciais ou industriais ou relativos a direitos de propriedade literária, artística ou científica.

Quanto à questão de saber se os limites constitucionais e legais do princípio em estudo são taxativos, ainda que numa primeira leitura e, tendo em conta o princípio da legalidade se possa dizer que sim, tal conclusão não poderá lograr. Assim, o princípio deverá sofrer restrições sempre que entrar em colisão com outros direitos liberdades e garantias, também constantes do bloco de legalidade, que devam sobressair na ponderação da administração.[18]

O Tribunal Constitucional já se pronunciou, concluindo que a reserva do nº 2 do art.º 268º "é uma remissão da Constituição para a lei e não uma exceção

14 Otero, Paulo; Direito do Procedimento Administrativo; Volume I; 1ª Ed.; Almedina; 2016; pág. 119.

15 Miranda, Jorge e Medeiros, Rui; Constituição Portuguesa Anotada; Tomo III; 1ª ed.; Coimbra Editora; 2007, pág. 601.

16 Canotilho, José Joaquim Gomes e MOREIRA Vital; Constituição Da República Portuguesa Anotada; Tomo II; 4ª Ed.; Coimbra Editora; 2010; pág. 824.

17 Moncada, Luís S. Cabral; Código do Procedimento Administrativo Anotado; 2ª Ed.; Quid Juris; 2017; pag. 125.

18 Otero, Paulo; Direito do Procedimento Administrativo; Volume I; 1ª Ed.; Almedina; 2016; pág. 121.

constitucional a normas constitucionais.[19]"

2.2. Lei de acesso aos documentos administrativos

O direito de acesso aos arquivos e registos administrativos, previsto na CRP e no CPA, é concretizado pela LADA, já referida anteriormente. Importa, pois, analisar o que aqui se dispõe para ter uma imagem completa do assunto em análise.

No seu artigo 2º, o legislador voltou a explicitar o princípio da administração aberta, realçando, contudo, a sua relação com os demais princípios da atividade administrativa, designadamente "os princípios da igualdade, da proporcionalidade, da justiça, da imparcialidade e da colaboração com os particulares".

Nesta lei, pela primeira vez, encontramos uma definição do conteúdo do direito de acesso a documentos administrativos – os documentos administrativos.[20]

Assim, de acordo com o legislador (art.º 3º nº 1 al. a)), estes documentos abrangem, "qualquer conteúdo, ou parte desse conteúdo, que esteja na posse ou seja detida em nome dos órgãos e entidades referidas no artigo seguinte, seja o suporte de informação sob forma escrita, visual, sonora, eletrónica ou outra forma material, neles se incluindo, designadamente, aqueles relativos a: i) Procedimentos de emissão de atos e regulamentos administrativos; ii) Procedimentos de contratação pública, incluindo os contratos celebrados; iii) Gestão orçamental e financeira dos órgãos e entidades; iv) Gestão de recursos humanos, nomeadamente os dos procedimentos de recrutamento, avaliação, exercício do poder disciplinar e quaisquer modificações das respetivas relações jurídicas".

Contudo, não nos basta esta definição legal para delimitar o âmbito de aplicação do princípio da administração aberta, impondo-se ainda analisar a fronteira negativa que resulta do nº 2 do art. 3º da Lei. Só aí se conclui o que é ou não um documento administrativo para este efeito. Assim, não são

19 Acórdão do TC nº 254/99; de 04-05-1999; proc. 456/97.

20 Pratas, Sérgio; A (nova) Lei de Acesso aos Documentos Administrativos; 1ª Ed.; Almedina; 2018; pág. 63.

documentos administrativos os documentos de natureza interna de que constem apenas notas pessoais, esboços ou apontamentos[21].

No que respeita aos sujeitos ativos deste direito, o art. 5º nº 1 concretiza a garantia da Constituição, clarificando, de acordo com a leitura atrás exposta, que *todos* são titulares do direito de acesso, incluindo pessoas coletivas privadas e cidadãos estrangeiros.[22] Referindo, de resto, na senda da Constituição, que tal requerimento não carece de fundamentação, sendo, pois, um direito de livre exercício.

Quanto aos sujeitos passivos do direito de acesso, não obstante alguns casos controversos na jurisprudência, a nova lei veio trazer uma maior clareza, incluindo no art. 4º uma definição das entidades abrangidas orientadas pelo conceito material de função administrativa, não restringindo o direito à noção clássica de administração.

A polémica surgia, essencialmente, a propósito das empresas públicas que não surgiam elencadas na anterior lei de 2007. Contudo, tanto a CADA, como a jurisprudência que a secundou entendeu que tais empresas integravam "um conceito amplo de Administração Pública", referindo ainda que o direito de acesso "não se restringe aos chamados atos de gestão pública, salvo se outra causa o impedir"[23].

Assim, vejamos a questão tal como ela é posta pelo Supremo Tribunal Administrativo (STA). Quando se referia à questão das empresas públicas e da sujeição à LADA, o STA afirma; "pode referir-se a uma noção ampla de administração em sentido material, que englobe toda a respectiva atividade em cumprimento da sua missão de «obtenção de níveis adequados de satisfação das necessidades da coletividade » (art. 4º DL nº 555/99, de 17/11) compreendendo quer a que levem a cabo com *ius imperii*, quer a que desenvolvam em paridade com os cidadãos, segundo as regras do direito privado".

E, mais à frente, *"*Temos, assim, na história da lei, um sinal inequívoco de que o legislador, para efeitos de aplicação do novo diploma, adotou o critério

21 Miranda, Jorge e MEDEIROS, Rui; Constituição Portuguesa Anotada; Tomo III; 1ª ed.; Coimbra Editora; 2007; Pág. 600.

22 Pratas, Sérgio; A (nova) Lei de Acesso aos Documentos Administrativos; 1ª Ed., Almedina, 2018, pág. 56

23 Parecer da CADA 164/2001; de 12-09-2001; Proc. 1455,1461.

amplo subjacente à posição da CADA segundo o qual as empresas públicas, mesmo quando agem segundo as regras do direito privado (art. 7º/1 DL 558/99 de 17.12), para prossecução da sua missão de "contribuir para o equilíbrio económico e financeiro do conjunto do sector público e para obtenção de níveis adequados de satisfação das necessidades da coletividade" (art. 4º DL 558/99) estão, indiretamente, a desenvolver uma atividade ou função materialmente administrativa e, por consequência, quis que a lei nova fosse aplicável a toda a sua atividade, (…)".[24]

Cumpre agora analisar o cerne da regulação constante da LADA. Com efeito, tratando-se de um documento administrativo, e não obedecendo a outro normativo especial, a regra será a disponibilização dos documentos, como resulta do art. 5º da LADA e do art. 268º nº 2 da CRP. Contudo, é necessário observar as restrições que, como já vimos, o princípio em estudo tem e a Constituição tolera[25].

2.2.1 Restrições ao livre acesso aos documentos administrativos

Na sequência dos diplomas já analisados, o art. 6º da LADA refere, como limites ao livre acesso, entre outros contidos em diplomas externos, (art. 7º nº1 da LADA: "Sem prejuízo das demais restrições legalmente previstas…") os documentos classificados e outros sob segredo de Estado (nº1), os direitos de propriedade intelectual (nº 2); os documentos administrativos respeitantes a procedimento administrativo não concluído (nº 3), o conteúdo de auditorias, inspeções, inquéritos, sindicâncias ou averiguações até ao fim do prazo para instauração de procedimento disciplinar (nº 4). A restrição prevista no nº 5 do art. 6º que é a mais frequente e a mais importante para o nosso estudo, pelo que a avaliaremos, com mais detalhe adiante.

No nº 7, referem-se ainda outros interesses juridicamente relevantes, como a eficácia da fiscalização ou supervisão (al. a)), a capacidade operacional ou segurança das forças de polícia e entidades consulares (al. b)), e outros

24 Acórdão do STA de 30-09-2009; Proc. 0493/09 e Acórdão do STA de 08/07/2009; Proc. 451/09

25 Pratas, Sérgio; A (nova) Lei de Acesso aos Documentos Administrativos; 1ª Ed.; Almedina; 2018; pág. 66.

danos "graves e dificilmente reversíveis a bens ou interesses patrimoniais de terceiros" merecedores de uma maior valoração do que os interesses protegidos pelo direito de acesso (al. c)).

De acordo com o nº 5, os documentos nominativos são, também, uma exceção ao livre acesso a documentos administrativos.

Em primeiro lugar, importa saber o que designa a lei por documentos nominativos.

Nos termos do art. 3º n.º 1 al. b) o legislador define-os como "documento que contenha dados pessoais, na aceção do regime jurídico de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" O presente conceito, remete, assim, para o Regulamento Geral de Proteção de Dados. Não nos demoraremos nesta definição, que será adiante estudada a propósito do princípio da proteção de dados pessoais.

Por agora, porque o conflito entre o direito de acesso aos arquivos e registos administrativos e o direto à proteção de dados pessoais, ainda vai ser tratado mais à frente no nosso estudo, importa fazer uma última exposição sobre a ponderação entre o regime geral de acesso e as exceções que o limitam.

Quanto a esta questão o STA tem-se pronunciado no sentido de que "O poder da Administração recusar o acesso à sua documentação é, assim, um poder vinculado aos princípios e objetivos fixados por lei, a ser exercido segundo os princípios da transparência e da proporcionalidade, que só deve ser invocado quando, o mesmo for indispensável para evitar prejuízos que não poderiam ser evitados doutra forma"[26].

Prosseguindo, "as referidas restrições só têm respaldo legal quando se não façam contra o disposto nos princípios da adequação e da proporcionalidade e que só serão legítimas quando a satisfação da pretensão formulada se traduzir na violação dos apontados direitos. Ou seja, também aqui, tanto o Requerente da informação como o órgão a quem ela é solicitada devem pautar o seu comportamento pelo interesse público sabendo-se que a satisfação deste, passa também pelo respeito dos direitos e interesses legítimos que podem ser

26 Acórdão do STA de 30/09/2009; Proc. 0493/09 disponível em <http://www.dgsi.pt/>

reflexamente atingidos pelo exercício do direito à informação"[27].

3. Princípio da proteção dos dados pessoais

3.1. Da sua previsão constitucional e inovação no CPA

O art. 18º do CPA, que consagra o princípio da proteção dos dados pessoais, é uma inovação de 2015, limitando-se a reconhecer aos administrados, não apenas o direito à proteção dos seus dados pessoais, como à "segurança e integridade dos suportes sistemas e aplicações, utilizados para o efeito, (...)". Porém não introduz elementos inovadores ao nível substantivo28. O essencial do regime deste direito encontra-se na CRP e no Direito da União Europeia com destaque para o Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27/04/2016 (RGPD) 29 e para a Lei nº 58/2019 que o concretiza a nível nacional.

No que à Constituição diz respeito, o artigo 26º nº 1 integra a reserva de intimidade da vida privada, contudo, seguindo a tendência para autonomizar o direito de proteção de dados do direito à proteção da vida privada (que de resto, estava também presente na Convenção Europeia dos Direitos do Homem (CEDH) Carta dos Direitos Fundamentais da União Europeia (CDFUE)), no contexto da administração, a disposição constitucional aqui relevante é o art.º 35º30.

A versão atual do artigo 35º da CRP resulta da quarta revisão Constitucional (1997). Aqui, o legislador constituinte reconhece e garante a autodeterminação informacional.

---

27 Acórdão do STA de 07/12/2011; Proc. 0671/11 disponível em <http://www.dgsi.pt/>

28 Pinheiro, Alexandre de Sousa; "A Proteção de Dados No Novo Código Do Procedimento Administrativo" in Comentários ao Novo Código de Procedimento Administrativo; Vol. I; 2018; AAFDL Editora; Pág. 335-362; Pág. 357.

29 Desde 25 de Maio de 2018, a disciplina de Proteção dos dados pessoais é objeto do Regulamento Geral de Proteção de Dados (Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016).

30 Pinheiro, Alexandre de Sousa; "A Proteção de Dados No Novo Código Do Procedimento Administrativo" in Comentários ao Novo Código de Procedimento Administrativo; Vol. I; 2018; AAFDL Editora; Pág. 335-362; Pág. 337.

Historicamente, o direito à proteção de dados pessoais derivou do princípio da dignidade humana e do direito ao livre desenvolvimento da personalidade, a partir dos quais o Tribunal Constitucional Federal Alemão retirou, hermeneuticamente, "uma garantia contra a recolha, armazenamento, utilização e transmissão dos seus dados pessoais" que não sejam admitidas pelo seu titular ou fundadas em interesse superior previsto na lei[31].

No contexto da jurisprudência constitucional germânica, o caso dos Censos Volkszählung-Urteil de 15 de dezembro de 1983, não só representa um leading case na matéria, como ilustra bem, como, no seu início, o princípio da proteção de dados pessoais surgia, essencialmente como uma garantia contra o poder da Administração Pública[32] perante o cidadão.

Podemos, aqui, claramente, identificar a natureza instrumental do direito à proteção de dados em relação a outros direitos fundamentais, nomeadamente o direito à reserva da vida privada e familiar previsto no art. 26º nº 1 da CRP, e como garantia da liberdade dos seus titulares.

Nesta vertente, o direito à proteção de dados pessoais é consagrado como um direito de natureza negativa que permite ao indivíduo opor ao Estado, o seu direito contra uma recolha e tratamento de dados que constitua uma intromissão ilegítima na sua vida privada[33].

Assim, e para uma melhor exposição da proteção constitucional, importa adotar a posição de Gomes Canotilho e Vital Moreira que segmentam o conteúdo do art. 35º em três direitos: o direito de acesso aos dados constantes dos registos informáticos (nº 1), bem como à sua retificação e atualização; o direito de sigilo dos dados pessoais face a terceiros (nº 4); o direito ao não tratamento de informático relativa a certos tipos de dados considerados sensíveis (nº 3). Por fim, a proibição do número nacional único permite garantir os direitos atrás referidos, dificultando a interconexão e o

31 Miranda, Jorge e Medeiros, Rui; Constituição Portuguesa Anotada; Tomo I; 1ª ed.; Coimbra Editora; 2005; Pág. 376.

32 Pinheiro, Alexandre de Sousa; "A Proteção de Dados No Novo Código Do Procedimento Administrativo" in Comentários ao Novo Código de Procedimento Administrativo; Vol. I; 2018; AAFDL Editora; Pág. 335-362; Pág. 337.

33 Miranda, Jorge e Medeiros, Rui; Constituição Portuguesa Anotada; Tomo I; 1ª ed.; Coimbra Editora; 2005; Pág. 381.

tratamento conjunto de várias categorias de dados.[34]

O respeito por estes direitos, exige, quando permitido o tratamento, entre outras ações: a transparência quanto aos dados recolhidos, o modo e período do seu tratamento, a identificação do seu responsável; a especificação das finalidades do tratamento; a limitação do tratamento de dados aos dados necessários para as finalidades especificadas que devem ser lícitas bem como a sua limitação no tempo, ao período necessário para os fins visados[35].

O direito à proteção de dados pessoais, porém, não se apresenta apenas como um mandato de abstenção dirigido ao Estado. O art. 35º impõe, ainda um dever de proteção e de garantia de respeito pelos privados, que caberá ao legislador infraconstitucional concretizar, bem como a criação de uma entidade administrativa independente para supervisionar o cumprimento da respetiva legislação. De resto, a mesma exigência é feita pelo art. 51º nº 1 do RGPD.

Da conjugação entre a Constituição, o RGPD e o art.º 3º da Lei nº 58/2019 tal entidade administrativa é a CNPD (Comissão Nacional para a Proteção de Dados).

A vertente prestacional do direito, assume-se, em nossa opinião, como a vertente mais importante do preceito, dada a proliferação, fora do círculo estadual, de ameaças contra a privacidade e a proteção dos dados pessoais pela multiplicação do poder tecnológico que os privados têm à sua disposição. Contudo, dado o contexto da nossa análise, centrar-nos-emos na sua aplicação no âmbito da função administrativa.

3.2. Da sua previsão no direito da União Europeia e em especial, no RGPD

3.2.1. Previsão no direito primário

Num primeiro momento, a tutela dos dados pessoais na União Europeia surge fortemente associada com o desenvolvimento do mercado único, visando

34 Canotilho, José Joaquim Gomes e Moreira, Vital; Constituição Da República Portuguesa Anotada; Tomo I; 4ª Ed.; Coimbra editora; 2007; pág. 551.

35 Canotilho, José Joaquim Gomes e Moreira, Vital; Constituição Da República Portuguesa Anotada; Tomo I; 4ª Ed.; Coimbra editora; 2007; pág. 552.

o fim, predominantemente económico, de garantir a segurança e o livre fluxo de dados pessoais entre os Estados Membros.

Tal fica patente, logo nos primeiros considerandos da Diretiva 95/46/CE[36] que demonstra preocupação com os direitos fundamentais, "Considerando que os sistemas de tratamento de dados estão ao serviço do Homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares (…)"[37] mas têm como principal objeto "o recurso ao tratamento de dados pessoais nos diversos domínios das atividades económicas e sociais"[38], preocupando-se especialmente com o "funcionamento do mercado interno", realçando que a livre circulação de mercadorias, das pessoas, dos serviços e dos capitais exige que os "dados pessoais possam circular livremente de um Estado Membro para outro, (…)"[39].

Este realce da perspectiva económica servia também como única forma de legitimar a intervenção da União neste domínio já que, o direito fundamental à proteção de dados pessoais constante da CDFUE só se tomaria igual peso aos Tratados, após o Tratado de Lisboa[40].

Assim, é no seguimento do Tratado de Lisboa, em 2009, que o princípio da proteção de dados pessoais adquire na União Europeia uma dimensão expressa e vinculativa.

Hoje, não só o Tratado sobre o Funcionamento da União Europeia (TFUE) reconhece este direito, como habilita a União a definir normas sobre o seu tratamento e com vista à sua proteção. Outro resultado do Tratado de Lisboa, foi a atribuição de força vinculativa ao art. 8º da CDFUE onde se encontra consagrado o direito fundamental à proteção de dados pessoais[41].

---

36 Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995

37 Considerando 2 da Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995.

38 Considerando 4 da Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995.

39 Considerando 3 da Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995.

40 Calvão, Filipa Urbano; "Garantia de direitos: a proteção de dados pessoais perante desafios tecnológicos" in Garantia de Direitos e Regulação: Perspetivas de Direito Administrativo; AAFDL Editora; 2020; Pág. 217-240; Pág. 221.

41 Calvão, Filipa Urbano; "Garantia de direitos: a proteção de dados pessoais perante desafios tecnológicos" in Garantia de Direitos e Regulação: Perspetivas de Direito Administrativo; AAFDL Editora; 2020; Pág. 217-240; Pág. 222.

Foi neste contexto legal, e face à crescente complexidade do tratamento de dados pessoais, bem como para fazer frente à utilização massiva de dados que as novas tecnologias vieram permitir às entidades públicas e privadas, que surgiu o RGPD, de forma a garantir um "quadro de proteção de dados sólido e mais coerente na União, (…)", bem como para "(...) assegurar um nível de proteção coerente e elevado das pessoas singulares (…)"[42]. Será este o regime que vamos agora estudar com mais detalhe.

3.2.2. Regime do RGPD e a Lei 58/2019 na Administração Pública

Quando na Constituição e no CPA remetem para a lei a concretização do regime de proteção dos dados pessoais, essa informação, deve, hoje, ser procurada no Regulamento Europeu que uniformizou a regulação a nível europeu.

Num primeiro momento, importa referir o conceito de dados pessoais[43] e do respetivo tratamento.

Ora, nos termos do art. 4º nº 1 do RGPD são dados pessoais qualquer informação respeitante a uma pessoa singular identificada ou identificável. Considerando-se identificáveis, neste âmbito, todos os que possam ser identificados direta ou indiretamente, em especial, por referência a um identificador como os exemplos constantes do artigo.

De seguida, o Regulamento define tratamento (art. 4º nº 2) como uma operação ou conjunto de operações, realizadas com dados pessoais ou um conjunto de dados pessoais, seja por meios automatizados ou não automatizados.

O tratamento de dados pessoais é perspetivado pelo legislador europeu, como de resto, já o era pela legislação dos Estados Membros e, em particular, pelo legislador português, como uma atividade potenciadora de riscos para os respetivos titulares.

Assim, e acompanhando as preocupações já expressas pelo "*Article 29 Data Protection Working Party"* em carta enviada à Comissão Europeia[44], o

42 Considerandos 7 e 10 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

43 De resto, essencial para uma leitura correta do conceito de documentos nominativos, no âmbito da alínea b) do nº 1 do art.º 3.º da LADA

44 Kohnstamm, Jacob; Comunicação do WP29 de 14-01-2011 para a Vice-Presidente

Regulamento adota uma abordagem baseada no risco, assumindo uma regulação predominantemente preventiva, orientada pelo princípio da precaução[45].

No contexto do atual Regulamento, a perspetiva de prevenção é consagrada pela imposição de deveres de ponderação de risco para os direitos, liberdades e garantias decorrentes do tratamento de dados, pelos responsáveis pelo tratamento de dados, prevendo-se o princípio da responsabilidade do responsável (art. 5º nº 2 do RGPD) e a obrigação de aplicar medidas que atenuem tal perigo[46]. Em adição, no considerando 78, o legislador Europeu impõe, ainda, que se considere o princípio da proteção de dados, "desde a conceção", bem como o princípio da proteção de dados pessoais por defeito. Tal previsão, longe de se destinar apenas aos entes privados, deve também ser levada em conta pelas entidades públicas, algo que salta à vista pela referência no considerando citado, aos contratos públicos.

Relevante, neste contexto é o art. 5º do RGPD, bem como no seu considerando 39 que consagram os princípios que constituem base do modelo de proteção de dados da União Europeia.

São eles, sucintamente, a licitude, lealdade e transparência do tratamento (al. a)), o princípio da limitação das finalidades (al. b)), a minimização dos dados (al. c)), a exatidão dos dados tratados (al. d)), a limitação da conservação (al. e)) integridade e confidencialidade (al. f)), seguidos do princípio da responsabilidade (nº 2)[47].

No art. 6º n.º 1º legislador europeu procedeu á densificação do princípio da licitude, atrás referido, indicando as condições a que o tratamento deve obedecer para ser lícito. Neste âmbito importa ainda referir o art. 9º para as categorias de dados especiais[48].

Viviane Reding, Comissária para a Justiça, Direitos Fundamentais e Cidadania.

45 Moniz, Graça Canto; "Breves Reflexões Sobre o Enquadramento Normativo Do Regulamento Geral De Proteção de Dados Pessoais" in Direito à Informação Administrativa e Proteção de Dados Pessoais, Coleção Formação Contínua; CEJ; 2021; Pág. 11-32; Pág. 27.

46 Considerando 74, 83 e 84; e nº 2 do art. 82º do RGPD

47 Para aprofundamento, ver: Kuner; Christopher, Bygrave, Lee A. e Docksey, Christopher; The EU General Data Protection Regulation (GDPR) A Commentary; Oxford; 2020; Pag. 309–320.

48 Kuner; Christopher, Bygrave, Lee A. e Docksey, Christopher; The EU General Data Protection Regulation (GDPR) A Commentary; Oxford; 2020; Págs. 325 e 365.

Uma vez coberto o paradigma regulatório que foi instituído pelo RGPD, importa fazer uma breve referência ao seu impacto na administração pública, em particular, no direito à informação administrativa.

O tratamento de dados pessoais, constantes de documentos oficiais na posse de autoridades ou organismos públicos tendo como fim a sua divulgação face ao princípio da administração aberta, está previsto no art. 86º do RGPD.

Naquele art. procura-se conciliar o princípio da administração aberta, também consagrado na CDFUE (art. 41º nº 1 al. b)), para além das Constituições dos Estados Membros, com o direito à proteção de dados pessoais.

Assim, no referido preceito, permite-se a divulgação dos dados pessoais, mas, atribuindo, no entanto, autonomia aos Estados membros para definir os respetivos regimes de acesso a documentos administrativos[49]. Pelo que, nesta matéria, sempre nos serviremos, para além do RGPD, quer da LADA, quer da lei nº 58/2019 de 8 de agosto que concretiza o regime Europeu, sendo de referir outros regimes especiais que aqui não falaremos.

A lei 58/2019 de 8 de agosto corresponde, então, à lei que veio exercer a função de execução do RGPD no ordenamento jurídico português, articulando, assim, o regime de proteção de dados pessoais assumido pela União Europeia e a regulação nacional em determinadas matérias, em que o legislador europeu permitiu ou impôs uma opção ao Estado Membro[50].

Nos termos do art. 2º nº 1 esta lei, aplica-se ao tratamento de dados, "independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante", ainda que o tratamento resulte de imposições legais ou seja feito na prossecução do interesse público. É, precisamente o caso da do princípio do arquivo aberto.

Pondo fim à sobreposição entre a LADA e a antiga Lei de Proteção de Dados do anterior contexto regulatório[51], o legislador limitou-se a fazer uma

---

49 Marques, Francisco Paes; Comentário ao art. 86º in Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019; Almedina; Lisboa; 2021; pág. 519

50 Calvão, Filipa Urbano; A Lei n.º 58/2019, de 8 de agosto: incongruências e insuficiências do RGPD; in Revista de Direito Administrativo; nº 8; 2020; AAFDL; Pág. 45-54; Pág. 45; e Art.º 1º da Lei 58/2019, de 8 agosto.

51 A CNPD na Deliberação n.º 241/2014 chegou a defender a revogação da LADA "de modo a restabelecer o regime legal uniforme de acesso aos dados pessoais em conformidade com a Constituição e as diretivas da União Europeia aplicáveis nesta matéria."

remissão para a LADA que, o que, contudo, se mostra redundante já que esta, remete para o RGPD, nomeadamente, no art. 1º nº 3 em que faz a sua ressalva, 10º nº 1 e alínea c) do art. 20º quanto à divulgação e reutilização de documentos.

4. Articulação entre o Princípio da Administração Aberta e o Princípio da Proteção de Dados Pessoais

Como atrás referimos, tanto o direito à proteção de dados pessoais previsto no art. 35º da CRP como o princípio da administração aberta, atributivo de um direito de acesso aos documentos administrativos (art. 268º nº 2 da CRP) são direitos fundamentais constitucionalmente acautelados. Em adição, também no Direito da União Europeia, se prevê, no art. 8º e na alínea b) do nº 1 do art. 41º da CDFUE, respetivamente, estes surgem como bens fundamentais.

Neste sentido, como refere Tiago Fidalgo de Freitas[52], o direito de acesso aos documentos administrativos tem de ser ponderado, casuisticamente, face a outros bens merecedores de tutela, in casu, o direito à proteção de dados pessoais, que dele possam eventualmente constar[53], respeitando, nomeadamente o princípio da proporcionalidade, relevante, quer a nível constitucional, quer na jurisprudência da União Europeia.

É esta ponderação que o legislador português procurou estabelecer na LADA, no que respeita ao regime dos documentos nominativos, cujo conceito atrás já expusemos. Assim, nos termos do art. 6 nº 5, têm o direito de acesso, para além dos titulares da informação nominativa, todos os que tenham a sua autorização, a qual deve ser explícita e específica, quer quanto aos dados a que se reporta, quer quanto á finalidade do tratamento (alínea a)), ou quem demonstrar ser titular de um "interesse pessoal, legítimo e constitucionalmente protegido", que deva prevalecer tendo em conta o princípio da proporcionalidade (alínea b)).

Por outro lado, no n.º 9 do art. 6º, determina-se que "(...) nos pedidos de acesso a documentos nominativos que não contenham dados pessoais

52 Freitas, Tiago Fidalgo de; As Restrições ao Direito à Informação Administrativa com Fundamento na Proteção de Dados Pessoais: Algumas Notas; in Direito à Informação Administrativa e Proteção de Dados Pessoais, Coleção Formação Contínua; CEJ; 2021; Pág. 113-126; Pág. 119 e 120.

53 Parecer da CADA nº 369/2021 de 16 de dezembro; Processo nº 565/2021

que revelem a origem étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, dados genéticos, biométricos ou relativos à saúde, ou dados relativos à intimidade da vida privada, à vida sexual ou à orientação sexual de uma pessoa, presume-se, na falta de outro indicado pelo requerente, que o pedido se fundamenta no direito de acesso a documentos administrativos".

Tal equilíbrio, de acordo com a CNPD, não se mostra, contudo, conforme ao RGPD. Para esta entidade, o regime da LADA não assegura a proteção dos direitos dos titulares de dados, de forma satisfatória face às exigências do legislador europeu.

Enquanto a alínea b) do nº 5 do art. 6º condiciona o acesso aos documentos nominativos à existência de um interesse direto, pessoal e constitucionalmente protegido, tal não tem reflexão no regime europeu, que, prevê no art. 6º os fundamentos para a licitude do tratamento de dados[54].

De acordo com o art. 6º nº 1 al. f) do RGPD, o tratamento será lícito, não havendo consentimento do seu titular, se tal for necessário para a concretização de um interesse legítimo prosseguido pelo responsável pelo tratamento (no caso o requerente) ou por terceiros, a não ser que prevaleçam os interesses ou direitos e liberdades fundamentais do titular.

Ora, perante esta preocupação levantada pela CNPD face à solução adotada pelo legislador português, importa verificar se a LADA protege de forma suficiente o direito à proteção de dados pessoais, não obstante a discrepância aparente entre as condições de acesso.

4.1. Fundamento para o tratamento de dados pessoais na LADA e no RGPD

Perante o exposto, é necessário proceder a uma comparação entre o "interesse direto, pessoal, legítimo e constitucionalmente protegido suficientemente relevante"[55] requerido pelo regime de acesso à informação administrativa e ambiental, e os "interesses legítimos prosseguidos pelo responsável pelo tratamento", previsto como condição de licitude pelo RGPD.

54 Parecer da CNPD; nº 20/2018; Proc. 6275/2018; Pág. 33.

55 Lei nº 26/2016, de 22 de agosto.

Ora, um conceito geral que defina o interesse exigido pela LADA, não consta nem da lei, nem dos pareceres da CADA nem na jurisprudência, sendo antes apurado casuisticamente.

Contudo, dos pareceres proferidos é possível retirar que o requerente deve apresentar uma razão, suficientemente relevante, para justificar a prevalência dos seus motivos diante dos diretos fundamentais do titular dos dados[56]. Tal vai de resto, de acordo com a orientação adotada pela jurisprudência de que a regra, nestes casos, deve ser a privacidade e a proteção de dados pessoais[57].

Seguindo esta posição, a CADA tem, perante os vários requerimentos, adotado um modelo de análise decomposto em duas fases, avaliando, num primeiro momento, se o motivo invocado para o acesso é ou não suficiente para facultar os dados, e, numa fase seguinte, indagando se da efetivação do direito de acesso não resultam prejuízos para o titular dos dados[58]. Vejamos o caso do RGPD.

Quanto ao art. 6º n.º 1 al. f) do RGPD, este deve ser interpretado como impondo a realização de um teste de ponderação, no qual os interesses legítimos do responsável pelo tratamento (no caso, o requerente dos documentos) serão contrapostos aos interesses e direitos do titular dos dados[59].

No que diz respeito ao interesse legítimo do responsável pelo tratamento, tal é entendido como um interesse lícito, definido de forma suficientemente clara, representando uma finalidade real e atual[60], sendo que o tratamento deve ser necessário às finalidades invocadas, não podendo existir outros meios menos invasivos da proteção de dados pessoais para a prossecução do mesmo fim[61].

---

56 Parecer da CADA nº369/2021; de 16-12-2021; Proc. 565/2021

57 Acórdão do TCAS de 22/01/2009; Proc. 04527/08; disponível em <http://www.dgsi.pt/>

58 Parecer da CADA nº 73/2017 de 14-02-2017; Proc. 45/2017.

59 WP29º; 'Parecer n.º 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva n.º 95/46/CE', de 9 abril de 2014, 844/14/PT WP 217; Pág. 36 e 37.

60 WP 29.º, 'Parecer n.º 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva n.º 95/46/CE', de 9 abril de 2014, 844/14/PT WP 217 Pág. 40

61 WP 29.º, 'Parecer n.º 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva n.º 95/46/CE', de 9 abril de 2014, 844/14/PT WP 217 Pág. 45

Num segundo momento, para que o tratamento possa ser considerado lícito ao abrigo do art. 6º nº 1 al. f), há que ponderar os "direitos e liberdades fundamentais do titular que exijam a proteção de dados pessoais", sendo que, no seguimento do que se afirmava na vigência da diretiva, todos os interesses relevantes da pessoa em causa devem ser tidos em conta[62].

Por último, a apreciação do tratamento, implica a realização do teste de ponderação, sendo que, para que o interesse legítimo do responsável se sobreponha ao direito do titular dos dados, o tratamento (no caso o acesso aos documentos nominativos) deve ser necessário e proporcional ao impacto nas pessoas afetadas.

O conceito de impacto deve ser entendido como abrangendo quaisquer resultados possíveis do tratamento da divulgação dos dados[63], tendo em conta, nomeadamente, a forma como os dados são tratados, as expectativas razoáveis do titular dos dados e o estatuto do responsável pelo tratamento e do titular de dados em causa.[64]

4.2. Harmonização dos fundamentos constantes da LADA e do RGPD

Resulta do art. 288º do TFUE, bem como do princípio do primado do Direito da União Europeia, que os regulamentos são obrigatórios, em todos os seus elementos, devendo, portanto, a legislação nacional abster-se de interferir na sua aplicação. Para além disto, em caso de incompatibilidade entre um regulamento e o direito nacional, o primeiro prevalece, com a desaplicação do direito nacional. Assim, deve a legislação nacional que o executa, ser interpretada conforme às pretensões uniformizadoras do RGPD.[65]

---

62 WP 29.º, 'Parecer n.º 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva n.º 95/46/CE', de 9 abril de 2014, 844/14/PT WP 217 Pág. 47

63 WP 29.º, 'Parecer n.º 06/2014; sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva n.º 95/46/CE', de 9 abril de 2014, 844/14/PT WP 217 Pág. 58

64 WP 29.º, 'Parecer n.º 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva n.º 95/46/CE', de 9 abril de 2014, 844/14/PT WP 217; Pág. 61 a 63

65 Cordeiro, António Barreto Menezes; Comentário ao Artigo 1º da Lei nº 58/2019 de 8 de agosto, in Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019; Almedina; 2021; Coimbra; Pág. 561 e 562.

Tendo em conta isto e a exposição que fizemos anteriormente, entendemos, como Tiago Fidalgo de Freitas, que não obstante a diferença de formulação, tanto a alínea b) do n.º 5 do art. 6º da LADA como a alínea f) do nº 1 do artigo 6º do RGPD se devem interpretar de forma equivalente, interpretando a disposição nacional à luz do normativo europeu[66].

Assim, vejamos, nos termos da LADA, apenas interesses constitucionalmente protegidos, podem fundamentar a restrição dos direitos do titular dos dados. Tal vai ao encontro do regime europeu, contando-se o exercício de direitos fundamentais, bem como interesses públicos, como um possível interesse legítimo para o tratamento dos dados.[67] Para além disto, a LADA, tal como, na interpretação do Grupo de Trabalho do Artigo 29, impõe uma ponderação orientada pelo princípio da proporcionalidade, aplicando o teste da ponderação.

Como exemplo desta prática pela nossa jurisprudência, importa referir o acórdão do TCAS de 27/07/2020[68] onde se refere que perante a ausência de autorização escrita, se havia de "verificar, como fez a sentença recorrida, qual o interesse direto pessoal, legítimo e constitucionalmente protegido suficientemente relevante no acesso solicitado pela requerente, ora recorrente, e sua a eventual preponderância à exigência de proteção dos dados pessoais em presença, nos termos da alínea b) do n.º 5 do citado art. 6°".

Neste contexto há, ainda, que referir o respeito pelo princípio da minimização dos dados previsto no art. 5º n.º 1 al. c) do RGPD, que encontra eco na obrigação da CADA de, nos termos do art. 6º nº 8 e 10º nº 5 da LADA, proceder ao expurgo dos dados que não relevem para a intenção do acesso[69]. Para além disto, os documentos nominativos não poderão ser reutilizados, nos termos do art. 20º al. C), exceto quando os dados pessoais possam ser anonimizados sem possibilidade de reversão, acautelando-se, assim, a

66 Freitas, Tiago Fidalgo de; As Restrições ao Direito à Informação Administrativa com Fundamento na Proteção de Dados Pessoais: Algumas Notas; in. Direito à Informação Administrativa e Proteção de Dados Pessoais, Coleção Formação Contínua; CEJ; 2021; Pág. 113-126; Pág. 124

67 WP 29.º, 'Parecer n.º 06/2014; Pág. 53

68 Acórdão do TCAS, de 27-07-2020; Proc. 133/20.7BECTB; disponível em <http://www.dgsi.pt/>

69 Parecer da CADA n.º 298/2021 de 02-11-2021; Proc. 733/2021.

existência de salvaguardas adequadas prevista na alínea e) do nº 4 do art. 6º do RGPD.

De resto, apenas o princípio da limitação das finalidades, previsto no art. 5º nº 1 al. b) e 6º nº 4 do RGPD parece levantar problemas. Tal princípio impõe que a finalidade do novo tratamento de dados seja compatível com aquela para a qual eles foram inicialmente recolhidos.

Na medida em que a LADA, se concentra no critério da legitimidade do fim visado pelo requerente do acesso, no tratamento de dados, é necessário recorrer aos critérios do 6º nº 4 do RGPD, a fim de avaliar da compatibilidade entre o fim para o qual os dados foram inicialmente recolhidos e a finalidade do tratamento que lhes será dado posteriormente.

Assim, na alínea a) volta-se a reiterar a necessidade de garantir a limitação de finalidades, sendo que para avaliar da compatibilidade entre os diferentes fins, o legislador europeu refere, de forma exemplificativa e não exaustiva[70] que devem ser tidos em conta, o contexto da recolha dos dados pessoais (al. b)) bem como a avaliação dos riscos envolvidos no tratamento posterior e sua retenção[71]. O considerando 50 introduziu, ainda, o critério das expectativas razoáveis do titular dos dados.

Tudo considerado, podemos então concluir que, o tratamento de dados para o exercício do direito de acesso a documentos administrativos nominativos em conformidade da LADA é lícito nos termos do artigo 6º nº 1 al f) e nº 4 do RGPD.

Assim, esta não consideração pelo princípio da limitação das finalidades por parte do regime da LADA, não se afigura como uma incompatibilidade, como parece sugerir a CNPD no parecer que antecedeu a lei 58/2019,[72] mas antes como uma lacuna que carece de ser integrada ao abrigo do RGPD. Acompanhamos, contudo, a crítica subjacente de que esta referência deveria, constar do texto da lei de acesso aos documentos administrativos, a fim de

---

70 Cordeiro, António Barreto Menezes; Comentário ao Artigo 6º nº 4 do RGPD, in Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019; Almedina; 2021; Coimbra; Pág. 119

71 Kuner; Christopher, Bygrave, Lee A. e Docksey, Christopher; The EU General Data Protection Regulation (GDPR) A Commentary; Oxford; 2020; Pag. 342.

72 Parecer da CNPD; nº 20/2018; Proc. 6275/2018; Pág. 33.

simplificar o trabalho do intérprete-aplicador.

Tal preocupação, ganha uma maior acuidade, atendendo à falta de recursos e formação da administração pública nos temas da proteção de dados e segurança de informação. De resto, uma lei especial mais simples não só "facilitaria" o trabalho do funcionário (que não teria de interpretar normas de diversos diplomas de fonte nacional e europeia) como também na prática, iria garantir menos erros que afetem os direitos fundamentais dos titulares.

É de notar que a integração desta formulação da LADA não é necessária, num plano substantivo, contudo, na prática poderá significar uma maior proteção dos direitos fundamentais dos administrados e garantir o pleno respeito pelo princípio da proteção de dados.

5. Nota Conclusiva

No nosso trabalho, procedemos à exposição de dois importantes princípios da atividade administrativa, o princípio da administração aberta, instrumental para a transparência da administração, e o princípio da proteção de dados, cuja importância tem vindo a crescer, sobretudo, a partir da aprovação do RGPD e a sua entrada em vigor em 2018.

Apesar do carácter breve da análise, o estudo de ambos os regimes, sobretudo, na parte final, relativamente às condições de acesso aos documentos nominativos definidas pela LADA e às condições de licitude do tratamento de dados pessoais estabelecidos pelo RGPD, permitiu desconstruir a tese da CNPD de que a regulação da LADA era incompatível com o regime regulamentar, embora tenha também procurado salientar que o regime nacional carece de ser integrado e interpretado em face do RGPD, dado o carácter de lex specialis deste diploma em relação ao regulamento.

Desta forma, embora não se corrobore o parecer da CNPD, dever-se-á salientar a necessidade de atualizar o regime de acesso aos documentos nominativos, de forma a incorporar as exigências do RGPD, não porque tais regulações se mostrem incompatíveis, mas para uma maior facilidade de aplicação pelos agentes da Administração Pública.

Os conflitos entre os princípios de proteção de dados e os deveres de AML no âmbito do tratamento de dados pelas instituições financeiras

CHRISTIANO AGUIAR *

Resumo: No âmbito da prevenção ao branqueamento de capitais e financiamento do terrorismo, as instituições financeiras tratam os dados das pessoas singulares envolvidas em relações de negócio e transações ocasionais com base no cumprimento de uma obrigação jurídica a que as instituições financeiras estão sujeitas. No entanto, este tratamento de dados envolve conflitos entre os princípios previstos no RGPD e os deveres impostos pelo regime de prevenção ao branqueamento de capitais e financiamento do terrorismo, designadamente o princípio da transparência contra o dever de não divulgação das informações, o princípio da minimização dos dados contra o dever de diligência quanto à clientela e o princípio da limitação da conservação dos dados contra o dever de conservação dos dados

Palavras-chave: *prevenção ao branqueamento de capitais; princípios de proteção de dados; conflitos entre RGPD e Diretiva AML.*

Abstract: In the context of the prevention of money laundering and terrorist financing, financial institutions process the data of individuals involved in business relationships and occasional transactions based on compliance with a legal obligation to which financial institutions are subject. However, this

* Advogado e Data Protection Officer no Banco de Investimento Global, S.A. Mestre em Direito (Especialidade de Direito de Empresa) na Universidade de Lisboa e Pós-Graduando em Direito da Proteção de Dados no Centro de Investigação de Direito Privado. Certificado pela Irish Computer Society – ICS

data processing involves conflicts between the principles provided for in the GDPR and the obligations imposed by the anti-money laundering and terrorist financing legal framework, namely the principle of transparency against the prohibition of disclosure of information, the principle of data minimization against the duty of customer due diligence and the principle of data storage limitation against the duty of data record-retention.

Keywords: *prevention of money laundering; data protection principles; conflicts between GDPR and AML Directive.*

1. Introdução

A proteção dos dados das pessoas singulares é um direito fundamental previsto no art. 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia (UE), e as regras relativas à proteção destes dados, nomeadamente quanto ao seu tratamento e à sua livre circulação, estão estabelecidas no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, mais conhecido como Regulamento Geral Sobre a Proteção de Dados (RGPD).

Ao abrigo do RGPD, os dados pessoais devem ser tratados de forma lícita e equitativa, assegurando a transparência necessária para que os titulares destes dados saibam quem é o responsável pelo tratamento, as suas finalidades, o seu fundamento de licitude e como os direitos do titular podem ser exercidos, entre outras informações.

Num âmbito distinto, a UE assegura a proteção da integridade, da estabilidade e da reputação do seu sistema financeiro e do seu mercado interno, que podem ser prejudicados pelos fluxos de dinheiro com origem ilícita. O branqueamento de capitais e o financiamento do terrorismo são problemas significativos que devem ser tratados ao nível da UE, pelo que releva estabelecer medidas preventivas para o efeito.

A prevenção do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo é regulada pela Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015,

mais conhecida como Diretiva AML (*Anti-Money Laundering*)[1], parcialmente transposta para o regime jurídico português através da Lei n.º 83/2017, de 18 de agosto, ou Lei de Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo (LBCFT)[2].

O RGPD e a Diretiva AML são regimes jurídicos que possuem interesses opostos que serão desenvolvidos no presente trabalho, nomeadamente quanto aos princípios aplicáveis ao tratamento dos dados pessoais, que por vezes entram em conflito com os deveres impostos pelo regime de prevenção ao branqueamento de capitais.

2. O RGPD e a Prevenção ao Branqueamento de Capitais

2.1. O tratamento de dados pessoais no âmbito da prevenção ao branqueamento de capitais

A solidez, a integridade e a estabilidade das instituições financeiras[3] poderão ser gravemente comprometidas pelos esforços dos criminosos e dos seus cúmplices para dissimular a origem do produto do crime, dando origem ao branqueamento de capitais[4].

1 Por se tratar da principal Diretiva AML atualmente em vigor, será o diploma mais estudado no presente trabalho. Sobre a evolução histórica completa do regime da prevenção ao branqueamento de capitais, ver Machado, Miguel (2020), "Deveres antibranqueamento de capitais: De onde vieram, quais são e como vão evoluir (do "4G" ao "5G")", Novos Estudos sobre Law Enforcement, Compliance e Direito Penal, Coord. Maria Fernanda Palma et al, pp. 259-351. Coimbra: Almedina.

2 No âmbito da regulamentação setorial, releva destacar o Aviso n.º 2/2018 do Banco de Portugal, publicado em 26 de setembro de 2018, que regulamenta as condições de exercício, os procedimentos, os instrumentos, os mecanismos, as formalidades de aplicação, as obrigações de prestação de informação e os demais aspetos necessários a assegurar o cumprimento dos deveres preventivos do branqueamento de capitais e do financiamento do terrorismo, no âmbito da atividade das entidades financeiras sujeitas à supervisão do Banco de Portugal.

3 Considerar-se-á a definição de instituição financeira prevista no n.º 2 do art. 3.º da Diretiva AML e na alínea v) do n.º 1 do art. 2.º da LBCFT. Sem prejuízo do termo "instituição financeira", que será adotado no presente trabalho, sublinhe-se que a Diretiva AML estabelece distinções entre a instituição de crédito e a instituição financeira, não obstante ambas sejam consideradas "entidades obrigadas" para efeitos de aplicação deste diploma.

4 Conforme o n.º 3 do art. 1.º da Diretiva AML, entende-se por branqueamento de capitais os comportamentos a seguir descritos, quando praticados intencionalmente: "a) A conversão ou transferência de bens, com conhecimento de que esses bens provêm de uma atividade criminosa ou da participação numa atividade dessa natureza, com o fim de encobrir ou dissimular a sua origem ilícita ou de auxiliar quaisquer pessoas implicadas nessa atividade

É relevante identificar todas as pessoas singulares que detêm a propriedade ou o controlo de uma pessoa coletiva, permitindo às instituições financeiras identificar o beneficiário efetivo[5] desta pessoa coletiva e as diligências que deverão ser adotadas para prevenir o branqueamento de capitais. A necessidade de dispor de informações exatas e atualizadas sobre o beneficiário efetivo é um fator essencial para rastrear os agentes do crime, que de outro modo poderão dissimular a sua identidade numa estrutura societária[6].

Neste âmbito, as instituições financeiras adotam medidas baseadas no risco para compreender a estrutura de propriedade e controlo do cliente, incluindo a recolha de documentos, dados ou informações fiáveis sobre a cadeia de participações ou de controlo. Ao abrigo do n.º 1 do art. 13.º da Diretiva AML, as medidas de diligência quanto à clientela (*Customer Due Diligence*)[7] incluem:

---

a furtarem-se às consequências jurídicas dos atos por elas praticados; b) O encobrimento ou a dissimulação da verdadeira natureza, origem, localização, utilização, circulação ou propriedade de determinados bens ou de direitos sobre esses bens, com conhecimento de que tais bens provêm de uma atividade criminosa ou da participação numa atividade dessa natureza; c) A aquisição, detenção ou utilização de bens, com conhecimento, no momento da sua receção, de que provêm de uma atividade criminosa ou da participação numa atividade dessa natureza; e d) A participação num dos atos a que se referem as alíneas a), b) e c), a associação para praticar o referido ato, a tentativa e a cumplicidade na sua prática, bem como o facto de facilitar a sua execução ou de aconselhar alguém a praticá-lo." No ordenamento jurídico português, o branqueamento constitui um crime previsto no art. 368.º-A do Código Penal (Decreto-Lei n.º 48/95).

5 Conforme o n.º 6 do art. 1.º da Diretiva AML, o beneficiário efetivo é "a pessoa ou pessoas singulares que, em última instância, detêm a propriedade ou o controlo do cliente e/ou a pessoa ou pessoas singulares por conta de quem é realizada uma operação ou atividade (...)". Em Portugal, a Lei n.º 89/2017, de 21 de agosto, aprovou o Regime Jurídico do Registo Central do Beneficiário Efetivo (RJRCBE), e a entidade gestora do Registo Central do Beneficiário Efetivo (RCBE) é o Instituto dos Registos e do Notariado, I. P. (IRN), que designa os serviços que, em cada momento, reúnem as melhores condições para assegurar os procedimentos relativos a este registo.

6 Conforme o Considerando 14 da Diretiva AML.

7 Pizarro, Sebastião Nóbrega (2016), "Manual De Compliance", p.36. Braga: Nova Causa Edições Jurídicas. Na prática de Compliance bancário, este dever de identificação e diligência quanto à clientela diz respeito ao procedimento Know Your Customer (KYC). Também designado de Know Your Client, este procedimento surgiu no âmbito da aprovação do Consolidated KYC Risk Management pelo Comité de Basileia, em outubro de 2004, o qual defendia a necessidade de as instituições bancárias aplicarem políticas e procedimentos de KYC, na perspetiva de garantir a segurança e transparência nas transações.

a) A identificação do cliente e a verificação da respetiva identidade, com base em documentos, informações ou dados obtidos junto de fonte independente e credível;
b) A identificação do beneficiário efetivo e a adoção de medidas razoáveis para verificar a sua identidade para que a entidade obrigada obtenha conhecimento satisfatório;
c) A avaliação e, se necessário, a obtenção de informações sobre o objeto e a pretendida natureza da relação de negócio;
d) A realização de uma vigilância contínua da relação de negócio, incluindo o exame das operações realizadas no decurso dessa relação, a fim de assegurar que tais operações são consentâneas com o conhecimento que a entidade obrigada tem das atividades e do perfil de risco do cliente, incluindo, se necessário, da origem dos fundos.

Assim, uma vez prestados os elementos de identificação por parte do cliente, é-lhe atribuído um nível de risco que pode ser baixo, médio ou alto, o que se vai refletir no tipo de diligência a adotar, podendo tal diligência ser simplificada quando o grau de risco for baixo, nos termos dos art. 15.º a 17.º da Diretiva AML, ou reforçada quando o grau de risco for elevado, de acordo com os critérios estabelecidos nos art. 18.º a 24.º da Diretiva AML[8].

Nos ordenamentos jurídicos sujeitos à Diretiva AML, cada Estado-Membro toma as medidas adequadas para identificar, avaliar, compreender e mitigar os riscos de branqueamento de capitais e de financiamento do terrorismo a que está exposto, bem como quaisquer preocupações conexas em matéria de proteção de dados, e mantém atualizada essa avaliação do risco, conforme determina o n.º 1 do art. 7.º da Diretiva AML.

8 A lista não exaustiva dos fatores e tipos indicativos de risco potencialmente mais baixo está prevista no Anexo II da Diretiva AML, e a lista não exaustiva dos fatores indicativos de situações com um risco potencialmente mais elevado está prevista no Anexo III do mesmo diploma. Ambas as listas dividem os fatores de risco em 3 tipos, nomeadamente os seguintes: (i) fatores de risco de cliente, (ii) fatores de risco associados ao produto, serviço, operação ou canal de distribuição, e (iii) fatores de risco geográfico. Não obstante, as instituições financeiras, ao determinarem o alcance das medidas de diligência quanto à clientela, devem tomar em consideração as seguintes variáveis de risco previstas no Anexo I da Diretiva AML: "i) O objeto de uma conta ou relação; ii) O nível de bens depositados por um cliente ou o volume das operações efetuadas; iii) A regularidade ou a duração da relação de negócio".

O ordenamento jurídico português prevê que as instituições financeiras, antes do estabelecimento de uma relação de negócio ou da realização de qualquer transação ocasional, devem identificar os clientes e seus respetivos representantes, exigindo sempre a apresentação de documentos de identificação válidos. No caso de pessoas singulares, esta identificação ocorre mediante recolha e registo dos seguintes elementos identificativos: i) Fotografia; ii) Nome completo; iii) Assinatura; iv) Data de nascimento; v) Nacionalidade constante do documento de identificação; vi) Tipo, número, data de validade e entidade emitente do documento de identificação; vii) Número de identificação fiscal ou, quando não disponha de número de identificação fiscal, o número equivalente emitido por autoridade estrangeira competente; viii) Profissão e entidade patronal, quando existam; ix) Endereço completo da residência permanente e, quando diverso, do domicílio fiscal; x) Naturalidade; xi) Outras nacionalidades não constantes do documento de identificação[9].

Numa breve análise, percebe-se que o tratamento de dados pessoais no regime da prevenção ao branqueamento de capitais envolve uma grande quantidade de dados do cliente bancário, do seu representante e do beneficiário efetivo, tendo as instituições financeiras, como será visto adiante, o dever de conservar tais dados por longos períodos conforme o regime jurídico aplicável.

2.2 Fundamento de licitude aplicável ao tratamento

No âmbito da prevenção ao branqueamento de capitais, as instituições financeiras assumem a posição de responsáveis pelo tratamento prevista no n.º 7 do art. 4.º do RGPD, uma vez que determinam as finalidades e os meios de tratamento dos dados pessoais dos clientes bancários, seus respetivos representantes e beneficiários efetivos, que são os titulares destes dados.

O fundamento de licitude para este tratamento está previsto na alínea c) do n.º 1 do art. 6.º do RGPD, na medida em que o tratamento dos dados dos clientes bancários e/ou beneficiários efetivos é necessário para o *cumprimento de uma obrigação jurídica* a que a instituição financeira está sujeita.

9 Conforme alínea a) do n.º 1 do art. 24.º, n.º 1 do art. 25.º, e art. 26.º, sem prejuízo dos procedimentos complementares previstos no art. 27.º, todos da LBCFT.

Sublinhe-se que o tratamento dos dados realizado com base nesse fundamento de licitude considera os seguintes requisitos previstos na alínea c) do n.º 1 do art. 6.º do RGPD e no n.º 3 do mesmo artigo:

(i) O tratamento deve ser *necessário*: a necessidade existe na medida em que a lei assim a determine, pelo que a determinação da necessidade pressupõe uma interpretação prévia da lei[10];

(ii) O cumprimento de uma *obrigação jurídica* a que o responsável pelo tratamento esteja sujeito: a expressão obrigação jurídica deverá ser interpretada com o sentido de obrigação legal, pelo que o fundamento da alínea c) será sempre uma disposição legislativa e não uma disposição contratual. A obrigação legal tanto pode ter origem numa lei formal, como numa lei material[11], não sendo necessário uma lei específica para cada tratamento de dados concretos, ou seja, a mesma lei pode impor mais do que uma obrigação legal[12];

(iii) A obrigação jurídica deverá ser definida pelo *direito da UE*[13] ou

10 Menezes Cordeiro, António Barreto (2021), "Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019", p.113, Coord. António Barreto Menezes Cordeiro. Coimbra: Almedina. Ver ainda o Considerando 45 do RGPD.

11 Sobre os dois conceitos, ver Sousa, Miguel Teixeira de (2012), "Introdução ao estudo do Direito", p.145ss. Coimbra: Almedina.

12 Ibidem.

13 Para além da Diretiva AML, releva mencionar a Diretiva (UE) 2019/1153 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa à utilização de informações financeiras e de outro tipo para efeitos de prevenção, deteção, investigação ou repressão de determinadas infrações penais; a Diretiva (UE) 2018/1673 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativa ao combate ao branqueamento de capitais através do direito penal; o Regulamento (UE) 2018/1672 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo ao controlo das somas em dinheiro líquido que entram ou saem da União Europeia; a Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo; o Regulamento Delegado (UE) 2018/1108 da Comissão, de 7 de maio 2018, que estabelece normas técnicas de regulamentação sobre os critérios de nomeação e funcionamento dos pontos de contacto centrais dos emitentes de moeda eletrónica e dos prestadores de serviços de pagamento; a Diretiva (UE) 2016/2258 do Conselho, de 6 de dezembro de 2016, relativa ao acesso às informações anti-branqueamento de capitais por parte das autoridades fiscais; o Regulamento Delegado (UE) 2016/1675 da Comissão, de 14 de julho de 2016, que procede à identificação dos países terceiros de risco elevado que apresentam deficiências estratégicas; e o Regulamento (UE) 2015/847 do Parlamento Europeu e do Conselho, de 20 de maio 2015, que estabelece as informações sobre o ordenante que devem acompanhar as transferências de fundos.

pelo *direito de um Estado-Membro*[14]: a disposição legal que deverá ser cumprida pelo responsável pelo tratamento não pode ter origem no Direito de um Estado terceiro. Além disso, o direito da UE ou do Estado-Membro poderá especificar as condições gerais do RGPD que regem a legalidade do tratamento dos dados pessoais, estabelecer regras específicas para determinar os responsáveis pelo tratamento, o tipo de dados pessoais a tratar, os titulares dos dados em questão, as entidades a que os dados pessoais podem ser comunicados, os limites a que as finalidades do tratamento devem obedecer, os prazos de conservação e outras medidas destinadas a garantir a licitude e equidade do tratamento[15]; (iv) A obrigação jurídica deverá responder a um objetivo de *interesse público* e ser *proporcional* ao objetivo legítimo prosseguido: os dois elementos deste requisito não dizem respeito ao tratamento de dados *per se*, mas sim à delimitação das competências legislativas concretizadoras da UE e dos Estados-Membros, não podendo qualquer um destes extravasar a letra e o espírito do RGPD. Por exemplo, o n.º 3 do art. 57.º da LBCFT reconhece expressamente a prevenção e o combate ao branqueamento de capitais e ao financiamento do terrorismo como um domínio de proteção de um interesse público importante, incluindo no que se refere aos tratamentos de dados pessoais efetuados com base na LBCFT.

Assim, as instituições financeiras estão sujeitas aos deveres preventivos previstos na Diretiva AML, sem prejuízo da legislação aplicável à matéria em cada Estado-Membro, pelo que tratam os dados pessoais neste âmbito com base no cumprimento de uma obrigação jurídica, ao abrigo da alínea c) do n.º 1 do art. 6.º do RGPD.

14 É o caso, por exemplo, da LBCFT (Portugal), da Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (Espanha), do Décret n° 2020-118 du 12 février 2020, renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme (França), e do Decreto Legislativo 21 novembre 2007, n. 231, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (Itália).

15 Conforme o Considerando 45 do RGPD.

No caso da LBCFT, o n.º 1 do art. 57.º autoriza as instituições financeiras a realizar os tratamentos de dados pessoais necessários ao cumprimento dos deveres de prevenção do branqueamento de capitais e do financiamento do terrorismo. Esta é a finalidade exclusiva deste tratamento, não podendo tais dados ser posteriormente tratados para quaisquer outros fins, incluindo os fins comerciais, conforme prevê o n.º 2 do art. 57.º do mesmo diploma.

As categorias de dados pessoais a que as instituições financeiras estão autorizadas a tratar para cumprimento dos deveres preventivos são aquelas previstas no n.º 1 do art. 58.º da LBCFT, nomeadamente as seguintes:

> a) Dados de identificação e de contacto, bem como dados fiscais e profissionais e as qualificações do respetivo titular, incluindo os seguintes elementos: i) Elementos previstos no art. 24.º (mencionadas no capítulo anterior); ii) Elementos caracterizadores das atividades prosseguidas; iii) Elementos relativos aos cargos políticos ou públicos que sejam ou já tenham sido exercidos[16]; iv) Elementos relativos a relações de parentesco e de afinidade[17], bem como a relações societárias, comerciais,

16 As pessoas politicamente expostas, mais conhecidas na prática como PEP (Politically Exposed Person), bem como os membros da família e as pessoas conhecidas como estreitamente associadas às mesmas, impõem sobre as instituições financeiras um dever de diligência reforçada quanto à clientela previsto nos art. 20.º a 22.º da Diretiva AML. O n.º 9 do art. 3.º da Diretiva AML define que as «Pessoas politicamente expostas» são as "pessoas singulares a quem estão ou foram cometidas funções públicas proeminentes, a saber: a) Chefes de Estado, chefes de Governo, ministros, ministros-adjuntos e secretários de Estado; b) Deputados ou membros de órgãos legislativos similares; c) Membros dos órgãos de direção de partidos políticos; d) Membros dos supremos tribunais, dos tribunais constitucionais e de outros órgãos judiciais de alto nível cujas decisões não sejam passíveis de recurso, salvo em circunstâncias excecionais; e) Membros dos tribunais de contas e dos órgãos de administração dos bancos centrais; f) Embaixadores, encarregados de negócios e oficiais de alta patente das forças armadas; g) Membros de órgãos de administração, de direção ou de supervisão de empresas públicas; h) Diretores, diretores-adjuntos e membros do conselho de administração ou pessoas que exercem funções equivalentes numa organização internacional."

17 O n.º 10 do art. 3.º da Diretiva AML define que os «Membros da família» incluem "a) O cônjuge, ou pessoa equiparada ao cônjuge, de pessoa politicamente exposta; b) Os filhos e respetivos cônjuges, ou pessoas equiparadas a cônjuge, de pessoa politicamente exposta; c) Os pais de pessoa politicamente exposta;", e o n.º 11 do mesmo artigo define que «Pessoas conhecidas como estreitamente associadas» podem ser "a) Qualquer pessoa singular que seja notoriamente conhecida por ter a propriedade efetiva conjunta de pessoas coletivas e de centros de interesses coletivos sem personalidade jurídica, ou por manter outro tipo de relações comerciais estreitas com pessoa politicamente exposta; b) Qualquer pessoa singular que tenha a propriedade efetiva de uma pessoa coletiva ou de um centro de interesses coletivos sem

profissionais ou sociais relevantes;

b) Dados financeiros e bancários, incluindo os relativos: i) Ao crédito e à solvabilidade dos respetivos titulares; ii) Aos rendimentos ou outros bens relacionados com os titulares dos dados;

c) Informação sobre a finalidade e a natureza da relação de negócio;

d) Informação sobre a origem e o destino dos fundos ou outros bens movimentados no âmbito de uma relação de negócio ou da realização de uma transação ocasional;

e) Informação sobre os demais elementos caracterizadores de todas as operações realizadas no decurso de uma relação de negócio ou no contexto de uma transação ocasional;

f) Informação sobre suspeitas de infrações penais[18], da prática de contraordenações ou de outras atividades ilícitas, incluindo a seguinte: i) Informação sobre comunicações de operações suspeitas efetuadas pela própria entidade obrigada ou por outras entidades comunicantes; ii) Informação sobre outras participações efetuadas às autoridades competentes; iii) Informação disponibilizada pelas autoridades competentes;

g) Informação sobre decisões que apliquem penas, medidas de segurança, coimas, sanções acessórias ou outras sanções pela prática dos atos a que se refere a alínea anterior.

Portanto, o tratamento dos dados pessoais no âmbito da prevenção ao branqueamento de capitais será lícito desde que a instituição financeira realize esse tratamento com base no cumprimento de uma obrigação jurídica prevista no direito da UE ou no direito de um Estado-membro a que a instituição financeira esteja sujeita.

---

personalidade jurídica notoriamente conhecidos como tendo sido constituídos em benefício de facto da pessoa politicamente exposta."

18 A proteção dos dados das pessoas singulares no que diz respeito ao tratamento, pelas autoridades competentes, para efeitos de prevenção, investigação, deteção ou repressão de infrações penais, é regulado pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Em virtude disto, o RGPD exclui, através de seu art. 2.º, n.º 2, alínea d), o tratamento de dados pessoais para estes efeitos do seu âmbito de aplicação material.

3. Os conflitos entre os princípios do RGPD e os deveres de prevenção ao branqueamento de capitais e financiamento do terrorismo

É fundamental que o regime AML esteja alinhado com a plena observância do quadro legal existente para a proteção de dados, na medida em que certos aspetos da aplicação do regime AML envolvem a recolha, a análise, o armazenamento e a partilha de dados pessoais.

Para tentar encontrar as respostas a tais preocupações opostas, as Diretivas, regulamentos, leis e avisos setoriais normalmente limitam-se a fazer referências genéricas à proteção de dados, questionando-se a proporcionalidade dos meios e as finalidades dos dados exigidos para combater o branqueamento de capitais e outros tipos de crimes[19].

As autoridades e/ou organismos independentes, nomeadamente os 4 citados a seguir, tentam alinhar os dois regimes jurídicos sob estudo: Comité Europeu para a Proteção de Dados **(**CEPD**)** ou *European Data Protection Board* **(**EDPB**)**[20], Autoridade Europeia para a Proteção de Dados (AEPD) ou *European Data Protection Supervisor* **(**EDPS**)**[21], Grupo de Ação Financeira

---

19 Machado, Miguel (2020), "Deveres antibranqueamento de capitais: De onde vieram, quais são e como vão evoluir (do "4G" ao "5G")", Novos Estudos sobre Law Enforcement, Compliance e Direito Penal, Coord. Maria Fernanda Palma et al, pp. 316. Coimbra: Almedina.

20 Considerando os 4 seguintes documentos:

(i) Declaração sobre a proteção dos dados pessoais tratados no quadro da prevenção do branqueamento de capitais e do financiamento do terrorismo, adotada em 15 de dezembro de 2020 pelo CEPD. Disponível em: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_20201215_aml_actionplan_pt.pdf>

(ii) Letter from Andrea Jelinek (Chair of the EDPB) to Ms. Mairead McGuiness (European Commissioner for Financial services, financial stability and Capital Markets Union) and Mr. Didier Reynders (European Commissioner for Justice), sent on 19 May 2021. Disponível em: <https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf>

(iii) Guidelines 10/2020 on restrictions under Article 23 GDPR, adotadas em 13 de outubro de 2021 pelo CEPD. Disponível em: <https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf>

(iv) Parecer 14/2011 sobre questões de proteção dos dados ligadas à prevenção do branqueamento de capitais e ao financiamento do terrorismo, adotado em 13 de junho de 2011 pelo GT29. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_pt.pdf>

21 Considerando os 2 seguintes documentos:

(i) Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, adotada em 23 de julho de 2020 pelo EDPS. Disponível em: <20-07-23_edps_aml_opinion_en.pdf> (europa.eu), e

(GAFI) ou *Financial Action Task Force* (FATF)[22], e Autoridade Bancária Europeia ou *European Banking Authority* (EBA)[23].

De um modo geral, estas diretrizes, opiniões, recomendações e pareceres sublinham que os procedimentos adotados para cumprimento dos deveres preventivos do branqueamento de capitais devem ter em consideração a proteção dos dados das pessoas singulares envolvidas, mas nem todos destes documentos possuem termos que efetivamente esclarecem as dúvidas que surgem no cotidiano das instituições financeiras.

Na prática, a avaliação dos conflitos é casuística, pelo que requer uma análise cuidadosa que pondere os princípios do RGPD e os deveres preventivos de branqueamento de capitais a que as instituições financeiras estão obrigadas.

Sem prejuízo da existência de outros conflitos entre os princípios do RGPD e o regime AML, o presente trabalho estudará três conflitos comuns neste âmbito, designadamente (i) o princípio da transparência contra o dever de não divulgação das informações, (ii) o princípio da minimização dos dados

---

(ii) Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals, adotada em 22 de setembro de 2021 pelo EDPS. Disponível em: <https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf>

22 Considerando os 3 seguintes documentos:

(i) International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, adotado em 2012 e atualizado em outubro de 2021 pela FATF. Disponível em: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

(ii) Private Sector Information Sharing, adotado em novembro de 2017 pela FATF. Disponível em: Private-Sector-Information-Sharing.pdf (fatf-gafi.org), e (iii) Stocktake on Data Pooling, Collaborative Analytics and Data Protection, adotado em julho de 2021 pela FATF. Disponível em: <https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborativeanalytics-data-protection.html>

23 Considerando os 2 seguintes documentos:

(i) Orientações relativas aos Fatores de Risco de BC/FT, adotadas em 01 de março de 2021 pela EBA. Disponível em: <https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/revised-guidelines-on-ml-tf-risk-factors#pane-new-7bdd87fb-e02f-492a-99d6-129449e3cf9d> e

(ii) Draft on Regulatory Technical Standards under Article 9a (1) and (3) of Regulation (EU) n. 1093/2010 setting up an AML/CFT central database and specifying the materiality of weaknesses, the type of information collected, the practical implementation of the information collection and the analysis and dissemination of the information contained therein, adotadas em 06 de maio de 2021 pela EBA. Disponível em: <https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-countering-financing-terrorism/regulatory-technical-standards-central-database-amlcft-eu>

contra o dever de diligência quanto à clientela e (iii) o princípio da limitação da conservação dos dados contra o dever de conservação dos dados.

3.1 Princípio da transparência contra o dever de não divulgação das informações

O art. 5.º do RGPD consagra os princípios relativos ao tratamento de dados pessoais, e prevê na alínea a) do n.º 1 deste art. que os dados pessoais são "*objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados*".

A transparência é um dos elementos há muito consagrados no direito da UE. Trata-se de criar confiança nos processos que afetam os cidadãos, fazendo com que estes compreendam e, se necessário, se oponham a esses processos. Trata-se igualmente de uma expressão do princípio da lealdade em relação ao tratamento dos dados pessoais enunciado no art. 8.º da Carta dos Direitos Fundamentais da UE[24].

Nos termos do RGPD, a transparência é uma obrigação abrangente[25], aplicável aos três seguintes domínios centrais:

(i) O fornecimento de informações aos titulares dos dados relacionado com o tratamento leal: por exemplo, a identidade e os contactos do

24 Sobre este princípio, ver também as Orientações relativas à transparência na aceção do Regulamento 2016/679, adotadas em 29 de novembro de 2017 pelo GT29. Disponível em: <https://ec.europa.eu/newsroom/article29/items/622227/en>

25 O Considerando 39 do RGPD prevê que "O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados. As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento. (...)".

responsável pelo tratamento, os contactos do encarregado da proteção de dados, as finalidades do tratamento, o fundamento de licitude para o tratamento, os destinatários ou categorias de destinatários dos dados pessoais, os prazos de conservação, as regras de transferência de dados para um país terceiro, se for o caso, de entre outras informações que possam interessar ao titular dos dados;

(ii) De que forma os responsáveis pelo tratamento comunicam com os titulares dos dados em relação aos direitos destes ao abrigo do RGPD: é suposto o responsável pelo tratamento fornecer ao titular as informações acima e qualquer comunicação de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, devendo tais informações ser prestadas por escrito ou por outros meios, incluindo, se for o caso, por meios eletrónicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios; e

(iii) De que forma os responsáveis pelo tratamento facilitam o exercício dos direitos dos titulares dos dados: o responsável pelo tratamento deve facilitar o exercício dos direitos do titular dos dados previstos nos art. 15.º a 22.º do RGPD, nomeadamente os direitos de acesso, retificação, apagamento, limitação do tratamento, portabilidade, oposição e não sujeição à decisões individuais automatizadas, incluindo definição de perfis.

Decorre também do n.º 2 do art. 5.º do RGPD que o responsável pelo tratamento tem sempre de poder comprovar que os dados pessoais são tratados de forma transparente em relação ao titular dos dados. Associado a isto, o princípio da responsabilidade exige a transparência das operações de tratamento para que os responsáveis pelo tratamento possam comprovar o cumprimento das suas obrigações nos termos do RGPD.

Assim, o conceito de transparência no RGPD, não sendo um conceito legalista, está centrado no utilizador e é concretizado através de requisitos práticos específicos que recaem sobre os responsáveis pelo tratamento e os subcontratantes em diversos artigos. Os requisitos práticos (em matéria de

informação) encontram-se definidos nos art. 12.º a 14.º do RGPD. Contudo, a qualidade, a acessibilidade e a compreensibilidade das informações são tão importantes como o conteúdo efetivo das informações em matéria de transparência, que devem ser fornecidas aos titulares dos dados.

O n.º 3 do art. 41.º da Diretiva AML (refletido no n.º 2 do art. 59.º da LBCFT) prevê que as instituições financeiras, antes de estabelecerem uma relação de negócio ou de efetuarem uma transação ocasional, devem fornecer aos novos clientes as informações exigidas no art. 13.º do RGPD. Essas informações incluem, em especial, um aviso geral quanto às obrigações legais das instituições financeiras em matéria de tratamento de dados pessoais para efeitos da prevenção do branqueamento de capitais e do financiamento do terrorismo. Para efeitos de cumprimento desta disposição legal, é prática comum entre os bancos constar este aviso geral na ficha de abertura de conta, remetendo as informações exigidas no art. 13.º do RGPD para as condições gerais de abertura de conta e/ou para a política de proteção de dados pessoais em vigor.

No entanto, em sentido contrário ao princípio da transparência consagrado pelo RGPD, o art. 39.º da Diretiva AML estabelece o *dever de não divulgação*[26], em que as entidades obrigadas, seus respetivos administradores e funcionários não podem divulgar ao cliente em causa, nem a terceiros, o facto de estarem a ser, irem ser ou terem sido transmitidas informações às Unidades de Informação Financeira (UIF)[27], designadamente as informações relativas ao conhecimento ou suspeita de que os fundos provêm de atividades criminosas,

26 Previsto no art. 54.º da LBCFT.

27 Entidades dos Estados-Membros que devem ser operacionalmente independentes e autónomas para recolher e analisar a informação que recebem com o objetivo de estabelecer ligações entre as operações suspeitas e as atividades criminosas a elas subjacentes, a fim de prevenir e combater o branqueamento de capitais e o financiamento do terrorismo. A alínea jj) do n.º 1 do art. 2.º da LBCFT define a UIF como a "unidade central nacional com competência para: i) Receber, analisar e difundir a informação resultante de comunicações de operações suspeitas nos termos da presente lei e de outras fontes quando relativas a atividades criminosas de que provenham fundos ou outros bens; e ii) Cooperar com as congéneres internacionais e as demais entidades competentes para a prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo". Em Portugal, a UIF está incluída na orgânica da Polícia Judiciária através da alínea b) do n.º 2 do art. 18.º do Decreto-Lei n.º 137/2019, de 13 de setembro, que aprovou a nova estrutura organizacional desta Polícia, como um serviço central diretamente dependente do diretor nacional. As suas competências estão descritas no art. 27.º do Decreto-Lei n.º 137/2019, de 13 de setembro, e no art. 82.º da LBCFT.

nem que está a ser ou pode vir a ser efetuada uma análise sobre branqueamento de capitais ou financiamento do terrorismo.

A divulgação da transmissão destas informações enviadas às UIF pode ser realizada junto das autoridades competentes e até entre as instituições financeiras, sendo ainda permitida para efeitos de aplicação da lei. O n.º 6 do art. 39.º da Diretiva AML autoriza as instituições financeiras a tentarem dissuadir um cliente de realizar uma atividade ilegal, sem que isso constitua uma violação ao dever de não divulgação, mas o cliente e seus respetivos representantes não podem tomar conhecimento de que estão a ser investigados com base no regime AML.

A não divulgação ao titular dos dados da transmissão destas informações entre as instituições financeiras é ancorada pela alínea b) do n.º 5 do art. 14.º do RGPD, uma vez que comunicar este tratamento de dados ao titular prejudicaria a obtenção dos objetivos desse tratamento (investigação da prática de branqueamento de capitais ou financiamento do terrorismo).

As Orientações relativas à transparência na aceção do RGPD, adotadas em 29 de novembro de 2017 pelo GT29, exemplificam o tema sob estudo através do seguinte caso prático[28]:

> "O Banco A está sujeito a uma obrigação ao abrigo da legislação relativa ao combate ao branqueamento de capitais de comunicar qualquer atividade suspeita relacionada com contas abertas no banco à autoridade responsável pela aplicação da lei competente no domínio financeiro. O Banco A recebe informações do Banco B (noutro Estado-Membro) de que o titular de uma conta deu instruções para transferir dinheiro para outra conta aberta no Banco A e que a operação parece suspeita. O Banco A transmite estes dados relativos ao titular da conta e às atividades suspeitas à autoridade responsável pela aplicação da lei competente no domínio financeiro. A legislação de combate ao branqueamento de capitais em causa qualifica como infração penal o facto de um banco que comunica estas informações «alertar» o titular da conta para a possibilidade de estar sujeito a investigações regulamentares. Nesta situação, o artigo 14.º, n.º 5, alínea b), é aplicável porque fornecer ao titular dos dados (o titular da conta no Banco A) as informações relativas ao artigo 14.º sobre o tratamento dos

28 Conforme p.37 das Orientações relativas à transparência na aceção do Regulamento 2016/679, adotadas em 29 de novembro de 2017 pelo GT29. Disponível em: <https://ec.europa.eu/newsroom/article29/items/622227/en>

> dados pessoais do titular da conta recebidos do Banco A iria prejudicar gravemente os objetivos da legislação, que inclui a prevenção deste tipo de «alertas». Contudo, quando abrem uma conta, todos os titulares de conta clientes do Banco A devem receber informações gerais acerca da possibilidade de os seus dados pessoais poderem vir a ser tratados para fins de combate ao branqueamento de capitais*"*.

Em decorrência do dever de não divulgação a que as instituições financeiras estão obrigadas, o n.º 4 do art. 41.º da Diretiva AML estabelece que os Estados-Membros adotam medidas legislativas que restrinjam, total ou parcialmente, o direito de acesso pelo titular dos dados aos dados pessoais que lhe dizem respeito, na medida em que essa restrição total ou parcial constitua uma medida necessária e proporcionada numa sociedade democrática e tenha devidamente em conta os legítimos interesses da pessoa em causa (i) para que a entidade obrigada ou a autoridade nacional competente possa desempenhar cabalmente as suas funções para efeitos da Diretiva AML, ou (ii) para evitar que se constitua um entrave aos inquéritos, análises, investigações ou procedimentos oficiais ou legais e garantir que não seja comprometida a prevenção, investigação e deteção do branqueamento de capitais e do financiamento do terrorismo.

No RGPD, a alínea d) do n.º 1 do art. 23.º estabelece que, para assegurar a prevenção, a investigação, a deteção ou a repressão de infrações penais, o direito da UE ou dos Estados-Membros pode limitar o alcance das obrigações e dos direitos previstos nos art. 12.º a 22.º e no art. 34.º, bem como no art. 5.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática[29].

---

29 O Considerando 19 do RGPD reconhece expressamente a importância dessa possibilidade de limitação na luta contra o branqueamento de capitais: "(...) Nos casos em que o tratamento de dados pessoais por organismos privados fica abrangido pelo presente regulamento, este deverá prever a possibilidade de os Estados-Membros restringirem legalmente, em determinadas condições, certas obrigações e direitos, quando tal restrição constitua medida necessária e proporcionada, numa sociedade democrática, para salvaguardar interesses específicos importantes, incluindo a segurança pública e a prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Tal possibilidade é importante, por exemplo, no quadro da luta contra o branqueamento de capitais ou das atividades dos laboratórios de polícia científica".

A alínea h) do n.º 2 do art. 23.º do RGPD complementa que estas medidas legislativas incluem, quando for relevante, disposições explícitas relativas ao direito dos titulares dos dados a serem informados da limitação, a menos que tal possa prejudicar o objetivo da limitação.

No ordenamento jurídico português, a limitação do direito de acesso do titular dos dados no âmbito da prevenção, deteção, investigação ou repressão de infrações penais se encontra refletida no art. 16.º da Lei n.º 59/2019, de 08 de agosto.

No âmbito específico da prevenção ao branqueamento de capitais e financiamento do terrorismo, esta limitação se encontra refletida no n.º 2 do art. 60.º da LBCFT, o qual estabelece que o direito de acesso aos dados pessoais pelo respetivo titular é negado nas situações previstas no n.º 1 do art. 54.º da LBCFT. É com base neste artigo que as instituições financeiras, bem como os membros dos respetivos órgãos sociais, os que nelas exerçam funções de direção, de gerência ou de chefia, os seus empregados, os mandatários e outras pessoas que lhes prestem serviço a título permanente, temporário ou ocasional, não podem revelar ao cliente ou a terceiros:

a) Que foram, estão a ser ou irão ser transmitidas as comunicações de operações suspeitas, comunicações sistemáticas de operações, comunicações realizadas no âmbito do dever de abstenção e as comunicações realizadas no âmbito do dever de colaboração com o Departamento Central de Investigação e Ação Penal da Procuradoria-Geral da República (DCIAP), a UIF, as demais autoridades judiciárias e policiais, as autoridades setoriais e a Autoridade Tributária e Aduaneira;

b) Quaisquer informações relacionadas com as comunicações acima, independentemente de elas decorrerem de análises internas da instituição financeira ou de pedidos efetuados pelas autoridades judiciárias, policiais ou setoriais;

c) Que se encontra ou possa vir a encontrar-se em curso uma investigação ou inquérito criminal, bem como quaisquer outras investigações, inquéritos, averiguações, análises ou procedimentos legais a conduzir pelas autoridades judiciárias, policiais ou setoriais;

d) Quaisquer outras informações ou análises, de foro ou interno ou externo, sempre que disso dependa: i) O cabal exercício das funções conferidas pela LBCFT às instituições financeiras e às autoridades judiciárias, policiais e setoriais; e ii) A preservação de quaisquer investigações, inquéritos, averiguações, análises ou procedimentos legais e, no geral, a prevenção, investigação e deteção do branqueamento de capitais e do financiamento do terrorismo.

Importa sublinhar que as hipóteses acima, que permitem às instituições financeiras negar o acesso aos dados pessoais requerido pelo titular dos dados, não prejudicam o direito de apresentação de queixa ou reclamação à Comissão Nacional de Proteção de Dados (CNPD) pelo titular dos dados, o recurso aos meios de tutela administrativa e o direito que tem o mesmo a obter reparação pelos danos sofridos, ao abrigo do art. 34.º da Lei n.º 58/2019, de 8 de agosto. Além disso, não prejudicam a verificação pela CNPD, oficiosamente ou a pedido do titular dos dados, da licitude do tratamento dos dados, bem como da informação àquele titular de que foram efetuadas todas as verificações necessárias e de que o tratamento de dados em causa reveste natureza lícita ou ilícita[30].

Em 13 de outubro de 2021, o CEPD adotou as *Guidelines 10/2020 on restrictions under Article 23 GDPR*[31], que visam fornecer orientações quanto à aplicação do art. 23.º do RGPD através de uma análise completa dos critérios para aplicar as restrições, as avaliações que têm de ser observadas, como os titulares dos dados podem exercer os seus direitos uma vez levantada a restrição e as consequências para as violações deste artigo.

O parágrafo n.º 24 da secção 3.3.2 das *Guidelines 10/2020 on restrictions under Article 23* GDPR, em comentário à alínea d) do n.º 1 do art. 23.º do

30 Sobre o recurso ao mecanismo da consulta prévia estabelecida no art. 36.º do RGPD, pelas instituições financeiras, para resolver o vácuo entre os princípios do RGPD e a abordagem baseada no risco do regime AML, ver Maxwell, Winston (2021), "The GDPR and Private Sector Measures to Detect Criminal Activity", Revue des Affaires Européennes - Law and European Affairs, p.24. Disponível em: <https://ssrn.com/abstract=3964066>

31 Guidelines 10/2020 on restrictions under Article 23 GDPR, adotadas em 13 de outubro de 2021 pelo CEPD. Disponível em: <https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf>

RGPD, considera que em certos casos o fornecimento de informações aos titulares dos dados que estão a ser investigados pode comprometer o sucesso dessa investigação, pelo que a restrição do direito à informação ou de outros direitos do titular dos dados pode ser necessária. O parágrafo n.º 24 considera expressamente que isto é relevante, por exemplo, no âmbito do combate ao branqueamento de capitais.

No entanto, o parágrafo n.º 25 pondera que as informações omitidas devem, em conformidade com a jurisprudência do Tribunal de Justiça da União Europeia (TJUE)[32], ser fornecidas uma vez e se já não for possível pôr em risco a investigação em curso. Segundo o parágrafo n.º 25, isto significa que deve ser dado um aviso específico de proteção de dados (feito à medida) ao titular dos dados o mais rapidamente possível, indicando os diferentes direitos, tais como acesso e retificação.

Em comentário à alínea h) do n.º 2 do art. 23.º do RGPD, os parágrafos n.ºs 64 a 67 da secção 4.7 das *Guidelines 10/2020 on restrictions under Article 23* GDPR, estabelecem critérios que poderão ser úteis às instituições financeiras que precisam apresentar uma resposta fundamentada a um pedido de acesso a dados pessoais em que o titular é uma pessoa que se encontra sob investigação. As orientações previstas nestes parágrafos entendem que os titulares dos dados devem, em regra, ser informados sobre a restrição ao seu direito à informação, sendo suficiente um aviso geral de proteção de dados para o efeito.

Nas fases muito preliminares de uma investigação, se o titular dos dados em causa solicitar informações sobre se está a ser investigado, o responsável pelo tratamento poderá decidir não conceder essas informações nesse momento – se esta restrição for lícita e estritamente necessária no caso específico para o que seria prejudicial ao objetivo da restrição.

Numa fase posterior, tal como após a conclusão da fase preliminar da investigação ou inquérito, os titulares dos dados em causa devem receber uma notificação específica de proteção de dados. Ainda é possível, nesta fase, que certos direitos continuem a ser restringidos, tais como o direito de acesso à informação sobre a abertura de uma investigação. Segundo os parágrafos

32 Opinion 1/15 of the CJEU (Grand Chamber) on the Draft PNR Agreement between Canada and the European Union, 26 July 2017, ECLI:EU:C:2017:592.

n.ºs 64 a 67, este facto deve ser indicado no aviso de proteção de dados, juntamente com a indicação de um período em que os direitos serão plenamente restabelecidos, se possível.

Em síntese, nos casos em que o fornecimento de informações ao titular dos dados prejudicar os objetivos do tratamento previstos no regime de prevenção ao branqueamento de capitais, o princípio da transparência consagrado pelo RGPD será mitigado pelo dever de não divulgação a que as instituições financeiras estão obrigadas, sem prejuízo de as restrições ao direito de acesso aos dados pelo titular serem levantadas numa fase posterior em que o fornecimento de informações não prejudique os objetivos do tratamento previstos no regime AML.

3.2 Princípio da minimização dos dados contra o Dever de Diligência quanto à clientela

A alínea c) do n.º 1 do art. 5.º do RGPD consagra o princípio da minimização dos dados ao estabelecer que os dados pessoais são "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados". Este princípio é composto pelos três seguintes pilares, que visam propósitos distintos, apesar de dificilmente autonomizáveis (em especial os dois primeiros)[33]:

(i) Adequação: impõe aos responsáveis pelo tratamento que circunscrevam a recolha e demais tratamentos a dados pessoais que se enquadrem nas finalidades prosseguidas. Os dados não relacionados ou inapropriados encontram-se, em princípio, excluídos.
(ii) Pertinência: este pilar circunscreve as atividades dos responsáveis a tratamentos que possam contribuir para a prossecução dessas finalidades. O termo "*relevant*", empregue na versão inglesa do RGPD, é mais feliz que o termo "pertinentes", empregue na versão portuguesa do RGPD.
(iii) Limitação: os dados pessoais são limitados ao que é necessário

33 Menezes Cordeiro, António Barreto (2021), "Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019", p.105, Coord. António Barreto Menezes Cordeiro. Coimbra: Almedina.

> relativamente às finalidades para as quais são tratados. Este pilar tem especial ligação com o princípio da limitação da conservação previsto na alínea b) do n.º 1 do art. 5.º do RGPD, que estabelece que os dados pessoais são "*recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades*".

Assim, o princípio da minimização dos dados tem por base a redução do tratamento dos dados pessoais ao mínimo necessário, pelo que o tratamento apenas será juridicamente aceitável se não existirem métodos alternativos menos intrusivos dos direitos dos titulares, tais como a anonimização prevista na alínea a) do n.º 1 do art. 32.º do RGPD, e a pseudonimização prevista no n.º 1 do art. 32.º do RGPD[34].

O n.º 1 do art. 41.º da Diretiva AML prevê que o tratamento de dados pessoais ao abrigo da mesma está sujeito ao cumprimento do RGPD, conforme transposição da Diretiva AML para o direito nacional, e o n.º 2 do mesmo artigo prevê que os dados pessoais são tratados pelas entidades obrigadas (como é caso das instituições financeiras) com base na Diretiva AML apenas para efeitos da prevenção do branqueamento de capitais e do financiamento do terrorismo, não podendo ser posteriormente tratados de forma incompatível com essas finalidades. Para o efeito, o n.º 2 do art. 41.º proíbe expressamente o tratamento posterior de dados pessoais com base na Diretiva AML para quaisquer outros fins, nomeadamente fins comerciais.

As medidas de luta contra o branqueamento de capitais incluem obrigações muito amplas e de grande alcance impostas às instituições financeiras, designadamente as obrigações de identificar os seus clientes, controlar as transações efetuadas através dos seus serviços e comunicar transações suspeitas, conforme se verifica através do n.º 1 do art. 13.º da Diretiva AML e dos art. 23.º e 24.º da LBCFT.

---

34 O Information Commissioner's Office (ICO), autoridade de controlo britânica no âmbito da proteção de dados, disponibiliza em seu site breves e interessantes orientações sobre o princípio da minimização dos dados, com exemplos práticos em diversos cenários de tratamento. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/.

O cumprimento do dever de identificação e diligência pelas instituições financeiras, é realizado através do tratamento de diversos tipos de dados pessoais, podendo a diligência ser reforçada conforme o risco que o cliente representa ao abrigo do regime AML. É difícil conciliar os deveres deste regime com o princípio da minimização dos dados, pois há fatores de risco que podem alterar a interpretação sobre os dados que são adequados, pertinentes e limitados ao que é necessário para prevenir o branqueamento de capitais e o financiamento do terrorismo no âmbito da abertura de uma conta bancária, bem como no âmbito da manutenção desta relação de negócio.

Tendo em consideração essas dificuldades, as autoridades e/ou organismos independentes tentam alinhar os dois regimes jurídicos. O Grupo de trabalho do art. 29.º para a Proteção dos Dados (GT29), grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do RGPD), adotou o Parecer 14/2011 sobre questões de proteção dos dados ligadas à prevenção do branqueamento de capitais e ao financiamento do terrorismo[35], sendo que, através deste Parecer, divulgou alguns entendimentos que relevam ao princípio da minimização de dados, designadamente os que seguem abaixo:

(i) A recolha sistemática de dados ao abrigo das obrigações de identificação e diligência quanto à clientela não deve ser vista como uma finalidade em si mesma, mas aplicada ao risco envolvido e deve ter em conta o princípio da minimização de dados. O requisito de fornecer dados relacionados com a identificação e diligência quanto à clientela deve sempre depender de uma avaliação de risco predefinida que tenha em conta diferentes fatores, tais como a situação do cliente, a natureza das transações, o produto financeiro ou os movimentos financeiros envolvidos;

(ii) O responsável pelo tratamento tem a obrigação de avaliar,

35 Parecer 14/2011 sobre questões de proteção dos dados ligadas à prevenção do branqueamento de capitais e ao financiamento do terrorismo, adotado em 13 de junho de 2011 pelo GT29. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_pt.pdf>

periodicamente, a exatidão dos dados, a necessidade de armazenar avaliações de risco mais antigas e a necessidade de continuar o tratamento de dados mais antigos relativos ao dever de identificação e diligência;
(iii) A recolha e subsequente tratamento de dados sensíveis para efeitos de prevenção do branqueamento de capitais é proibida, a menos que a necessidade desse perfil possa ser provada pela instituição financeira e desde que os legisladores e entidades reguladoras tenham também especificado salvaguardas adequadas, que devem ter como objetivo evitar a interpretação arbitrária das obrigações de identificação e diligência quanto à clientela pelas instituições financeiras. A simples referência a uma exceção legal ou a uma obrigação legal de perfilar é claramente inadequada, uma vez que não acrescenta quaisquer salvaguardas para processar dados sensíveis.

No dia 19 de maio de 2021, o CEPD, atento à necessidade de harmonizar o princípio da minimização de dados com o regime AML, apresentou as seguintes recomendações[36]:

(i) O regime de prevenção do branqueamento de capitais deve especificar o que é necessário e proporcional para cumprir as suas obrigações. Do ponto de vista da proteção de dados, é crucial inserir termos em cada obrigação deste regime que clarifiquem se os dados pessoais necessários para cumprir uma obrigação específica devem (apenas) ser recolhidos junto da pessoa em causa ou se outras fontes (por exemplo, entidades terceiras, públicas ou privadas) podem ou devem ser utilizadas. É igualmente necessário especificar, se for o caso, que tipos de categorias especiais de dados pessoais e/ou dados pessoais relativos a condenações e infrações penais poderão ou deverão ser tratados para cumprir essa obrigação específica;

36 Letter from Andrea Jelinek (Chair of the EDPB) to Ms. Mairead McGuiness (European Commissioner for Financial services, financial stability and Capital Markets Union) and Mr. Didier Reynders (European Commissioner for Justice), sent on 19 May 2021. Disponível em: <https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf>

(ii) Deve ser evitado o comportamento defensivo de entidades obrigadas (como é o caso das instituições financeiras), que as leva a enviar grandes quantidades de suspeitas não relevantes, gerando um elevado número de falsos positivos[37];

(iii) A nova legislação no âmbito AML deve conter, explicitamente, requisitos no sentido de que apenas os dados exatos e relevantes podem ser utilizados para os reportes. Estes requisitos devem também proibir a inclusão de dados pessoais relacionados com condenações penais e infrações que não sejam ligadas ao branqueamento de capitais ou ao financiamento do terrorismo.

Portanto, o princípio da minimização de dados consagrado no RGPD e o dever de diligência quanto à clientela previsto no regime AML devem ser abordados de forma equilibrada que, numa perspetiva de prevenção e combate a estas atividades criminosas, tenha em consideração os dados pessoais que são efetivamente adequados, pertinentes e limitados ao que é necessário para esta finalidade (cumprimento de deveres AML).

3.3. Princípio da limitação da conservação dos dados contra o Dever de conservação dos dados

A alínea e) do n.º 1 do art. 5.º do RGPD consagra o princípio da limitação da conservação dos dados ao estabelecer que os dados pessoais são "*conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais*

37 No contexto em causa, "falsos positivos" são reportes de transações baseados em conclusões equivocadas. Para seguir os padrões de KYC, as empresas devem proceder a uma monitorização contínua das suas relações de negócio para assegurar que os perfis de risco não mudaram de uma forma que exponha a empresa ao não cumprimento dos deveres antibranqueamento de capitais e aos danos reputacionais, mas isto é dispendioso para as instituições financeiras, na medida em que as soluções existentes produzem um grande número de falsos positivos devido à sua dependência de pesquisas manuais em múltiplas bases de dados que são difíceis de auditar. Os falsos positivos podem surgir porque pode haver milhares de nomes ou pontos de dados a combinar, produzindo centenas de resultados. Todos esses resultados têm de ser revistos manualmente para ver se são "falsos positivos" ou não. Ainda sobre o tema, ver o Glossário de Risco e Compliance da Dow Jones, disponível em: <https://www.dowjones.com/professional/risk/glossary/know-your-customer/false-positives/>

são tratados".

Com o término do período necessário para a prossecução dos fins determinados, os dados devem ser, o quanto antes, apagados. Cabe ao responsável pelo tratamento fixar os prazos para o apagamento ou para a revisão periódica da sua conservação, de forma a assegurar que os dados pessoais sejam mantidos apenas durante o período indispensável[38].

O art. 21.º da Lei n.º 58/2019, de 8 de agosto, densifica esta obrigação e prevê que o prazo de conservação de dados pessoais é o que estiver fixado por norma legal ou regulamentar ou, na falta desta, o que se revele necessário para a prossecução da finalidade. O n.º 3 deste artigo dispõe que quando os dados pessoais sejam necessários para o responsável pelo tratamento ou o subcontratante poderem comprovar o cumprimento de obrigações contratuais ou de outra natureza, os mesmos podem ser conservados enquanto não decorrer o prazo de prescrição dos direitos correspetivos. Cessada a finalidade que motivou o tratamento, inicial ou posterior, de dados pessoais, o responsável pelo tratamento deve proceder à sua destruição ou anonimização (n.º 4 do art. 21.º). Por fim, o n.º 5 deste artigo prevê que nos casos em que existe um prazo de conservação de dados imposto por lei, o direito ao apagamento previsto no art. 17.º do RGPD só pode ser exercido após o fim desse prazo.

A CNPD, através do Parecer 20/2018, adotado no dia 2 de maio de 2018, sobre a Proposta de Lei n.º 120/XIII/3.ª (Gov)[39], que acabou por ser adotada na Lei n.º 58/2019, de 8 de agosto, entendeu que o art. 21.º desvirtuou por completo o princípio da limitação da conservação dos dados, apresentando as seguintes críticas:

(i) Independentemente da definição de um prazo máximo de conservação, os dados pessoais devem ser eliminados ou tornados anónimos assim que estiver cumprida, no caso concreto, a finalidade do tratamento. A aplicação deste princípio não prejudica, obviamente, a necessidade de

38 Menezes Cordeiro, António Barreto (2021), "Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019", p.106, Coord. António Barreto Menezes Cordeiro. Coimbra: Almedina.

39 Parecer 20/2018, adotado no dia 02 de maio de 2018 pela Comissão Nacional de Proteção de Dados (CNPD), sobre a Proposta de Lei n.º 120/XIII/3.ª (Gov). Disponível em: https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2018&type=4&ent=

conservar dados quando haja lei que a tal obrigue. Porém, mesmo nestas circunstâncias, só devem ser conservados os dados que forem necessários para o cumprimento da obrigação legal e não outros que para o efeito não sejam necessários. Será o exemplo clássico de um tratamento de dados de gestão de clientes, em que é obrigatório a empresa manter os dados de faturação do cliente por um período de 10 anos para fins fiscais, daí não decorrendo o dever de conservar outros dados relativos ao cliente (tais como contactos, idade, consumos detalhados, interesses e preferências) se a relação contratual for terminada ao fim de dois anos;

(ii) O RGPD só admite ao Estado-Membro legislar dentro dos parâmetros definidos pelo Regulamento, quanto à conservação de dados durante períodos mais longos, quando em causa esteja a prossecução exclusiva de fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos. Contudo, outras vertentes foram reguladas de forma incompreensível nos n.ºs 1 e 4 do art. 21.º, o que é por si só violador do direito da UE, uma vez que o legislador nacional está adstrito a disciplinar apenas as matérias permitidas pelo Regulamento da UE;

(iii) O n.º 2 do art. 21.º dispensou com grande amplitude a limitação da conservação dos dados pessoais através da previsão de que esta conservação é lícita quando, pela natureza e finalidade do tratamento, não seja possível determinar antecipadamente o momento em que o mesmo deixa de ser necessário. Este texto permite a conservação ilimitada de dados pessoais *para qualquer finalidade*, por consideração ainda de um fator que não vem considerado no RGPD – o da *natureza* do tratamento.[40];

(iv) O n.º 3 do art. 21.º introduz uma finalidade autónoma e genérica ("*comprovar o cumprimento de obrigações contratuais ou de outra natureza*") que seria comum a todos os tratamentos e paralela às finalidades legítimas e determinadas de cada um deles, para dar cobertura

40A este propósito, convém recordar o considerando 39 do RGPD: "os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo". Esta relação estreita entre o princípio da limitação da conservação e o princípio da minimização dos dados, enquanto manifestação do princípio da proporcionalidade no âmbito dos tratamentos de dados, obriga a que os dados sejam apenas conservados enquanto forem necessários à prossecução da finalidade que está na base da sua recolha.

a uma conservação de dados por tempo quase ilimitado;

(v) O n.º 5 do art. 21.º opõe-se manifestamente ao teor do art. 17.º do RGPD, pois o facto de existir um prazo de conservação de dados legalmente fixado não impede o titular dos dados de exercer o seu direito ao apagamento, desde que reunidas as condições legais para esse apagamento, o que terá de ser apreciado casuisticamente.

Em conclusão, a CNPD recomendou a eliminação do art. 21.º da Lei n.º 58/2019, de 8 de agosto, com exceção do seu n.º 2, que poderá ser revisto. As críticas a este artigo, acima resumidas, dão alguma previsibilidade sobre o modo como a autoridade de controlo portuguesa aplicará o direito aos casos concretos que envolverem a conservação de dados pessoais.

No sentido contrário à limitação da conservação dos dados apenas durante o período necessário para as finalidades para as quais são tratados, o n.º 1 do art. 40.º da Diretiva AML impõe sobre as instituições financeiras um *dever de conservação* das informações e documentos tratados para efeitos de prevenção, deteção e investigação de possíveis atos de branqueamento de capitais ou financiamento do terrorismo. Esta disposição legal estabelece um prazo de conservação de 5 anos após o termo da relação de negócio com o cliente ou após a data de execução da transação ocasional, podendo os Estados-Membros autorizarem um período de conservação adicional de 5 anos após a realização de uma avaliação da necessidade e proporcionalidade.

Findo o prazo legal de conservação, os Estados-Membros devem assegurar que as entidades obrigadas apagam os dados pessoais, salvo disposição em contrário do direito nacional, que determina as circunstâncias em que as instituições financeiras podem ou devem conservar esses dados por mais tempo.

No ordenamento jurídico português, o art. 51.º da LBCFT estabelece que as informações e os documentos obtidos pelas instituições financeiras devem ser conservados por um período de 7 anos após o momento em que a identificação do cliente se processou ou, no caso das relações de negócio, após o termo delas.

O n.º 1 do art. 57.º da LBCFT autoriza as instituições financeiras a realizar o tratamento de dados pessoais necessários ao cumprimento dos deveres de prevenção ao branqueamento de capitais e financiamento do terrorismo, não podendo tais dados ser posteriormente tratados, com base no mesmo diploma, para quaisquer outros fins, incluindo fins comerciais.

O n.º 4 do art. 57.º da LBCFT dispõe que a finalidade do tratamento de dados exclusivamente para efeitos de cumprimento dos deveres de prevenção do branqueamento de capitais e financiamento do terrorismo não prejudica o tratamento de dados pessoais com base em outras disposições legais, nomeadamente no disposto na Lei n.º 58/2019, de 8 de agosto. Esta disposição é extremamente relevante para guiar as instituições financeiras, que poderão necessitar dos mesmos dados tratados no âmbito da LBCFT para finalidades previstas em outros regimes jurídicos, nomeadamente para cumprimento da lei fiscal[41].

A conservação de dados pessoais (não apenas para cumprimento do regime de prevenção ao branqueamento de capitais, mas também para outras finalidades) é um tema caro às instituições financeiras, uma vez que as relações de negócio que elas têm com seus clientes costumam ser duradouras, pelo que eliminar dados pessoais causa receios e é uma medida que encontra dificuldades operacionais de concretização em virtude da grande quantidade de dados tratados em diversos sistemas ao longo de muitos anos.

O CEPD recomenda que o regime AML especifique os dados pessoais que devem ser conservados e por quanto tempo, tendo em conta os princípios da necessidade e da proporcionalidade. Por exemplo, poderia ser feita uma distinção entre o período de conservação aplicável, por um lado, aos dados relacionados com transações executadas ou que tenham sido consideradas suspeitas e comunicadas à UIF e, por outro lado, o período de conservação aplicável aos dados relacionados com transações não suspeitas[42].

---

41 Designadamente o art. 52.º do Código do Imposto sobre o Valor Acrescentado (IVA).

42 Letter from Andrea Jelinek (Chair of the EDPB) to Ms. Mairead McGuiness (European Commissioner for Financial services, financial stability and Capital Markets Union) and Mr. Didier Reynders (European Commissioner for Justice), sent on 19 May 2021. Disponível em: https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf.

Com efeito, é complexo definir como as instituições financeiras devem proceder *após o fim do período legal de conservação* sem prejudicar o tratamento de dados baseados em outras obrigações legais ou que devam ser conservados ao abrigo de outros fundamentos de licitude. Não obstante, *durante o período legal de conservação*, uma boa prática a adotar pelas instituições financeiras será a pseudonimização dos dados pessoais e a disponibilização do acesso a estes dados exclusivamente aos colaboradores que, por motivos expressamente justificados, precisem tratar os dados dos clientes mesmo após o término da relação de negócio.

O conflito entre o princípio da limitação da conservação consagrado pelo RGPD e o dever de conservação dos dados previsto no regime AML, tal como os outros dois conflitos estudados no presente trabalho, levanta diversas questões e a expetativa é a de que as alterações legislativas e a divulgação de novas diretrizes e recomendações sejam capazes de clarificar as dúvidas existentes.

4. Conclusão

A luta contra o branqueamento de capitais e o financiamento do terrorismo é reconhecida como um domínio de proteção de um interesse público importante, tal como a proteção dos dados das pessoas singulares é reconhecida como um direito fundamental, pelo que os deveres impostos pela Diretiva AML precisam de ser cumpridos tendo em consideração os princípios consagrados pelo RGPD.

No âmbito do regime AML, as instituições financeiras tratam os dados das pessoas singulares envolvidas em relações de negócio e transações ocasionais ao abrigo da alínea c) do n.º 1 do art. 6.º do RGPD, ou seja, com base no cumprimento de uma obrigação jurídica a que estas instituições financeiras estão sujeitas na qualidade de responsáveis pelo tratamento.

Sem prejuízo da existência de outros conflitos entre os princípios do RGPD e o regime AML, o presente trabalho estudou três conflitos comuns neste âmbito, designadamente (i) o princípio da transparência contra o dever de não divulgação das informações, (ii) o princípio da minimização dos dados

contra o dever de diligência quanto à clientela e (iii) o princípio da limitação da conservação dos dados contra o dever de conservação dos dados.

O princípio da transparência, nos casos em que o fornecimento de informações ao titular dos dados prejudicar os objetivos do tratamento previstos no regime de prevenção ao branqueamento de capitais, será mitigado pelo dever de não divulgação a que as instituições financeiras estão obrigadas, sem prejuízo de as restrições ao direito de acesso aos dados pelo titular serem levantadas numa fase posterior em que o fornecimento de informações não prejudique os objetivos do tratamento previstos no regime de prevenção ao branqueamento de capitais.

O princípio da minimização de dados e o dever de diligência quanto à clientela a que as instituições financeiras estão obrigadas devem ser abordados de forma equilibrada, numa perspetiva de prevenção ao branqueamento de capitais e ao financiamento do terrorismo que tenha em consideração o tratamento dos dados pessoais que são efetivamente adequados, pertinentes e limitados ao que é necessário para esta finalidade.

O princípio da limitação da conservação e o dever de conservação dos dados deverão ser articulados à luz dos princípios da necessidade e da proporcionalidade, uma vez que o enquadramento legal aplicável, as diretrizes e recomendações neste âmbito não são suficientemente conclusivas quanto à forma ideal de conservar os dados pessoais tratados pelas instituições financeiras ao abrigo do regime AML, bem como quanto à forma ideal de eliminar esses dados findo o prazo legal de conservação.

A atualização do regime AML deve ser realizada com uma revisão da relação entre as medidas de prevenção ao branqueamento de capitais e os direitos à privacidade e à proteção de dados, pelo que uma articulação mais estreita entre os dois regimes jurídicos poderá beneficiar os dois lados.

O algoritmo no tecido empresarial: Das vicissitudes de contratação ao despedimento de trabalhadores – Uma arma nociva que necessita de ser desarmada?

FREDERICO VENTURA SEQUEIRA *

Resumo: A proliferação da inteligência artificial em contextos de tomada de decisão é saudada como uma bala de prata prometendo substituir a subjetividade humana por decisões objetivas e infalíveis, encobrindo males maiores que espelham a permissibilidade de decisões algorítmicas discriminatórias e arbitrárias, tomando a proporção de verdadeiras *WMDs*. Tendo presente o exponencial crescimento da adoção de algoritmos de *ML* nas relações laborais, propomo-nos exibir uma imagem mais nítida dos potenciais e efetivos malefícios juntamente com interrogações que carecem de respostas claras fruto do advento e da paulatina concretização da quarta Revolução Industrial, tentando desarmar algo que à primeira vista aparenta tratar-se de uma arma nociva que atua silenciosamente, procurando balizá-la e instruí-la de forma a (re)equilibrar os pratos da balança e conferir uma efetiva tutela aos candidatos a emprego e aos trabalhadores na iminência de mais um (grande) desafio que parece desafiar as condições da sua contratação, prestação do seu labor e cessação da sua atividade profissional, quer no que respeita ao trabalho tradicional, quer quanto às novas formas de o prestar. Para tal, defendemos uma reforma do uso de algoritmos de *ML* assente na sua regulação ético-jurídica, num processo completo e estruturado de auditoria, num efetivo direito à intervenção humana e num acesso informado aos critérios subjacentes à *ratio*

* Licenciado em Direito pela Faculdade de Direito da Universidade de Lisboa. Na mesma Instituição de ensino, frequenta o Mestrado em Direito e Ciência Jurídica, na especialidade de Direito Laboral, encontrando-se em fase de dissertação. O escrito que ora se apresenta corresponde, mutatis mutandis, ao relatório de Mestrado apresentado no âmbito da disciplina de Direito do Trabalho, sob a regência da Senhora Professora Doutora Maria do Rosário Palma Ramalho.

de uma decisão, permitindo imputar responsabilidades, reagir fundadamente e, desta forma, impedir esvaziamentos legislativos de conteúdo e normas simbólicas perante uma (nova) realidade que necessita de urgente adaptação uma vez que veio para ficar.

Palavras-chave: *decisões individuais automatizadas, algoritmos, discriminação e arbitrariedade, prova algorítmica, responsabilidade, RGPD, ser humano no comando, direito à explicação, direitos de PI e segredos comerciais*

Abstract: The proliferation of artificial intelligence in decision-making contexts is hailed as a silver bullet that promises to replace human subjectivity by objective and infallible decisions, covering up greater evils that reflect the permissibility of discriminatory and arbitrary algorithmic decisions, taking the proportion of real WMDs. Bearing in mind the exponential growth of the adoption of ML algorithms in labour relations, we intend to show a clearer image of the potential and effective harm together with questions that lack clear answers as a result of the advent and the gradual implementation of the fourth Industrial Revolution, trying to disarm something that, at first sight, seems to be a noxious weapon that acts silently, by seeking to restrict it and instruct it in order to (re)balance the scale and to provide an effective protection to job applicants and workers on the verge of another (big) challenge that appears to defy the conditions of their hiring, provision of their work and termination of their professional activity, either with regard to traditional work or the new ways of providing it. To this end, we advocate a reform of the use of ML algorithms based on ethical-legal regulation, a complete and structured auditing process, an effective right to human intervention and informed access to the criteria underlying the ratio of a decision, allowing responsibilities to be imputed, a well-founded and solid reaction and, in this way, preventing legislative emptiness of content and symbolic provisions in the face of a (new) reality that needs urgent adaptation once it's here to stay.

Keywords: *automated decision making; algorithms; discrimination and arbitrariness; algorithmic proof; accountability; GDPR; human in command; right to explanation; IP rights and trade secrets.*

1. Introdução

A importância da digitalização levou ao domínio da inteligência artificial (IA) em quase todas as esferas da nossa vida, onde se incluem as relações laborais, foco do nosso estudo. Mais concretamente, o algoritmo de *machine learning* (ML) apresenta traços de grande utilidade e genialidade no seio das empresas, porém, esse toque de magia vem rapidamente ofuscar os inúmeros problemas sensíveis que representa para o trabalhador ao trazer uma mão cheia de desafios que parecem não ter uma resposta clara à vista, pois a verdade é que os algoritmos parecem estar atualmente a substituir o empregador através da gestão digital do trabalho no que diz respeito a decisões chave da carreira do trabalhador que incluem a contratação, avaliação e despedimento. Algo que tem despertado a preocupação por parte de algumas entidades cujo juízo de prognose faz crer que tais práticas se tornarão ainda mais comuns, constituindo formas mais intensas na maioria das empresas espalhadas por todo o mundo. Tendo isto presente, propomo-nos trazer à discussão a exposição e tratamento de certas questões algorítmicas que nos parecem mais críticas no que concerne quer ao candidato a emprego, quer ao trabalhador, numa perspetiva internacional, europeia e comparatística, ao mesmo tempo que colocamos o ordenamento português a teste.

Num primeiro momento, fazemos um breve enquadramento acerca da relação do algoritmo de *ML* com a IA, no que consiste e quais as suas principais qualidades e defeitos, tratando de aferir, como ponto de partida, qual dos lados da balança tende a pesar e a ter mais impacto na relação laboral, i.e., se as vantagens que lhes estão associadas valem o sacrifício dos potenciais efeitos perniciosos e se, de facto, vale a pena auxiliarmo-nos da sua presença num contexto de emprego. Em seguida, fazemos uma análise teórico-prática na qual se dá ênfase e destaque a um punhado de casos reais da maior relevância que se inserem nos dois principais campos problematizantes do processo interno do

algoritmo e refletem questões ético-jurídicas: a discriminação e a parcialidade e arbitrariedade.

Ulteriormente, abordamos as decisões individuais automatizadas e o *profiling* no Regulamento Geral sobre a Proteção de Dados (RGPD) ao debruçarmo-nos sobre o seu art. 22º, norma inédita no que diz respeito a esta temática que a Lei n.º 58/2019, de 8 de agosto - Lei de Execução portuguesa - não foi capaz de dar seguimento, não deixando de tratar questões derivadas igualmente importantes e com soluções legislativas duvidosas que se colocam a montante e a jusante da relação laboral como: o direito à intervenção humana traduzido no facto da última palavra (dever) ser de um interveniente humano e não da máquina, bem como do direito do individuo a reagir e contestar a decisão tomada (pela máquina) perante um humano; o direito de acesso à informação e o nível de transparência possível de alcançar espelhado na difícil conciliação entre direitos de autor, *trade secrets* e *IP rights* que muitas vezes impedem que a *source code* algorítmica seja conhecida, pelo que, inserindo um algoritmo num contexto de *black box*, aferimos da possibilidade de se encontrar o melhor equilíbrio possível uma vez que, para uma pessoa alvo de *automated decision making* (ADM) poder reagir, fundamentando devidamente uma contestação informada, precisará de ter um mínimo de conhecimento acerca do critério subjacente a tal decisão que lhe foi desfavorável sob pena de não ter qualquer oportunidade de se defender.

Nesta esteira, caminhando para o final, o ordenamento português é também ele colocado a teste no que diz respeito às duas principais questões basilares do nosso estudo. Assim, após uma breve contextualização da tutela empregue no combate à discriminação, procura-se saber, por um lado, quem deverá ser responsável por uma decisão discriminatória tomada por um algoritmo de modo a evitar que a imputabilidade se dilua pelo facto da decisão ter sido tomada por uma máquina, e que tipo de responsabilidade deverá ser acionada perante tal situação caso não sejam criadas normas e institutos específicos para tratar destas novas questões que têm a IA como atriz principal; por outro lado, procura-se ainda saber como poderá a pessoa visada por tal decisão discriminatória reagir tendo em conta a nossa legislação laboral, destacando os casos de prestação de trabalho nas plataformas digitais onde o

problema parece colocar-se de forma ainda mais intensa.

Em jeito de conclusão, face a esta nova realidade algorítmica que tem ocupado cada vez mais e intensamente o seu espaço nas relações laborais, tentamos desarmar os algoritmos enquanto *weapons of "math" destruction (WMDs)* e contribuir para uma discussão tão atual e premente dos nossos dias ao propor um conjunto de *guidelines* que se focam nos quatro pontos críticos que, no nosso entender, exigem uma olhar atento e uma abordagem alternativa célere.

2. O Algoritmo e a sua ligação com a Inteligência Artificial.

2.1. Conceptualização e importância

Em termos generalistas, a Comissão Europeia entende por IA "os sistemas que dispõem de comportamento inteligente ao analisar o ambiente que os rodeia e, por conseguinte, tomar ações de modo a atingir propósitos específicos, sendo dotados de algum grau de autonomia"[1]. De uma forma mais restrita, poderíamos qualificá-la como a ciência e a engenharia de produzir máquinas inteligentes capazes de resolver tarefas que tipicamente requerem inteligência humana reproduzindo as suas idiossincrasias, daí que o termo "algoritmo" se identifique com algo que tem a capacidade de aprender a resolver determinado problema para o qual foi programado, apresentando respostas através de um conjunto de instruções e comandos que lhe são fornecidos[2], sintetizando e automatizando tarefas, sendo precisamente esta a ideia chave. A partir daí, podemos centrar-nos numa das suas modalidades, o *Machine Learning* enquanto terminologia utilizada para descrever o processo de fornecimento aos sistemas da capacidade de aprender e melhorar automaticamente a partir da

1 CE, Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the regions, "Artificial Intelligence for Europe", Brussels, 25.4.2018, COM (2018) 237 final, 2018. De igual modo, vide Fidalgo, Vítor Palmela, "Inteligência artificial e direitos de imagem", in: ROA, Ano 78, n.º 3-4, 2018, Lisboa, pp. 879-900, ao distinguir os conceitos de IA e tecnologia robótica usualmente confundidos, de onde poderemos concluir metaforicamente que a IA é a mente e a robótica o corpo.

2 Neste sentido, EUAFR, "Big data, algorithms and discrimination", 2018, disponível em: <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-in-brief-big-data-algorithms-discrimination_en.pdf>

experiência, sem ser explicitamente programado, onde se encontram os nossos algoritmos. James Zou utiliza uma frase muito simples, mas precisa, para os definir, referindo que "um algoritmo de *ML* é como um bebé recém-nascido a quem foi dado milhões de livros para ler sem lhe ensinarem o alfabeto"[3], o que certamente antecipa alguns problemas de relevo, levando Cathy O`Neil a qualificá-los como autênticas Armas de Destruição Matemática[4] (*WMD - Weapons of Math Destruction*) cujos três elementos característicos assentam na opacidade, no efeito de escala e nos danos provocados, que se traduzem **(a)** no respetivo alcance (*Widespread*), ao atingir um número considerável de pessoas e estando no centro das grandes e mais importantes decisões da vida de cada uma delas, como são a contratação e o despedimento; **(b)** no secretismo (*Mysterious*), pelo facto das pessoas não saberem o que são algoritmos, qual o seu papel na empresa ou como estão a ser avaliadas; **(c)** no efeito destrutivo (*Destructive*), pelo impacto arrasador que causam e por fomentarem a injustiça, dotados de critérios inquinados e poluídos.

De um modo simplificado, a conceptualização de um algoritmo assenta em duas características cruciais de modo a compreendermos o seu propósito: **(i)** A *data*[5], i.e., a reunião de informação e grandes quantidades de dados e

3 ZOU, James, "Removing gender bias from algorithms", The Conversation Journal, 2016, disponível em: ZOU, James, "Removing gender bias from algorithms", The Conversation Journal, 2016, disponível em: <https://theconversation.com/removing-gender-bias-from-algorithms-64721>

4 Acompanhamos de perto o valioso contributo da matemática O´Neil, Cathy, Weapons of Math Destruction - How Big Data Increases Inequality and Threatens Democracy, Crown Publishers, New York, 2016, pp. 15-32, que, enquanto uma das grandes pioneiras do estudo dos efeitos perniciosos do algoritmo, podemos defini-la como o nosso Neo ao nos relembrar de observar os "senhores" digitais invisíveis que nos rodeiam uma vez que vivemos cada vez mais numa *Matrix* de que a maioria de nós não (se a) percebe. A sigla utilizada pela A. deriva de um trocadilho na medida em que, originalmente, *WMD* é utilizada como forma de qualificar as *Weapons of Mass Destruction,* i.e., Armas de Destruição Maciça, e a A. reinventa-a, com o intuito de tomar uma posição.

5 Cfr. Goldenfein, Jake, "Algorithmic Transparency and Decision-Making Accountability: Thoughts for Buying Machine Learning Algorithms", in: Closer to the Machine: Technical, Social, and Legal aspects of AI, Office of the Victorian Information Commissioner (ed.), 2019, pp. 41-60, (p. 42). Como *e.g.*, vide o Report: Use of Workforce Analytics for Competitive Advantage, Society for Human Resource Management Foundation, "What´s next: future global trends affecting your organization", SHRM Foundation, 2016, p. 24 ao referenciar que a empresa *Nielson* usa a retenção do primeiro ano como métrica chave para avaliar se uma contratação foi bem-sucedida. Contudo é importante relembrar, tendo em conta a realidade do RGPD, o princípio da minimização dos dados (cfr. alínea c) do n.º 1 do

correspondência estatística padronizada, o *input* enquanto dados de entrada que vai espelhar o que aconteceu no passado, sendo por isso mesmo a característica *ex libris* da sua constituição e **(ii)** uma definição para o sucesso, i.e., qual o objetivo a atingir, o *output* enquanto gerador de um determinado resultado e decisão sem interferência humana, o que estamos à procura e o que queremos alcançar. Pois bem: na relação jurídico-laboral, a parte mais vulnerável (*in casu*, o candidato a emprego ou o trabalhador) não escolhe a dita definição do sucesso na empresa, sendo o seu contributo irrelevante para o conteúdo de um algoritmo que consiste sim em opiniões (*in casu*, do empregador) embutidas num código, que refletem a ideologia do seu criador dotado dos seus respetivos valores e desejos de modo a alcançar determinado resultado, ocorrendo, por isso, uma grande assimetria informativa (*e.g.*, em relação ao critério de contratação fornecido).

2.2. Da ilusão vantajosa aos reais efeitos perniciosos do seu uso

Os seus defensores pregoam alguns benefícios da sua presença cada vez mais acentuada nas relações laborais, pelo que destacamos os essenciais. *Primo*, integrando as novas tecnologias digitais, revelam-se como um recurso precioso na fase de recrutamento e seleção de trabalhadores, quer quando é feita diretamente pelo contratante, quer quando este recorre a prestadores de serviços externos, especialistas em recrutamento, auxiliando e permitindo que os recursos humanos (RH) tenham uma função cada vez mais estratégica e decisiva dentro das empresas[6], assistindo-se, por isso, a uma verdadeira gestão

art. 5º RGPD) devendo ser adequados, relevantes e limitados ao necessário em relação aos fins para os quais são processados sob pena do tratamento ser ilícito e constituir contraordenação muito grave prevista e sancionada nos termos da alínea a) do n.º 5 do art. 83º RGPD e da alínea a) do n.º 1, e do n.º 2 do art. 37º da Lei de Execução. Discutivelmente, isto não significa que os responsáveis pelo tratamento de dados devem recolher sempre o mínimo de dados possível, significa antes que a quantidade deve estar relacionada com a finalidade, desde que os dados sejam adequados. Não obstante, o efeito parece ser paradoxal: *Primo*, quanto mais dados forem utilizados para treinar o algoritmo, mais preciso poderá ser o output; *Secondo*, o processamento de uma baixa quantidade de dados, levando a um output inexato ou deficitário na qualidade seria algo inadequado se se tivesse de tomar uma decisão com consequências legais ou que afetasse significativamente determinado indivíduo.

6 Neste sentido, Clark, Melissa A., Makowsky, Libby & Zukiewicz, Marykate, "Implementation of the Teach For America Investing in Innovation Scale-Up", in: Mathematica Policy Research, Princeton, 2015, pp. 1-56, (pp. 11-16) e TODOLÍ-SIGNES,

automatizada do trabalho com cada vez maior expressão, de que é exemplo a contratação, a aferição dos tempos de produção, a designação e distribuição de tarefas, a avaliação do desempenho e até o despedimento dos trabalhadores. *Secondo*, é vista enquanto garante de ganhos de produtividade ao replicar operações naturais, o que permite desenvolver, produzir e acumular raciocínios aprendidos ao longo do tempo pelo ser humano com alto grau de velocidade e eficiência, otimizando o tempo dos recrutadores, tornando o processo de recrutamento menos custoso e mais eficiente, e reduzindo o tempo[7] e o risco de más contratações como demonstram os casos bem-sucedidos da *IBM*[8], da *Pymetrics*[9] e da *HireVue*[10]. *Terzo*, no que diz respeito ao *profiling* ou

Adrian, "Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection", in: European Review of Labour and Research, Vol. 25, n.º 4, 2019, pp. 1-17, (pp. 3-5).

7 Como indicam Bogen, Miranda & Rieke, Aaron, "Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias", in: Upturn, 2018, pp. 1-47, (pp. 6-7), "a maioria dos empregadores quer reduzir o tempo de contratação dado que quanto mais tempo for necessário para encontrar um candidato adequado, mais tempo e recursos são desviados de outras prioridades", receando perder candidatos para os seus concorrentes.

8 Segundo dados estatísticos do The Economist, "Big data and hiring - Robot recruiters: How software helps firms hire workers more efficiently", 2013, disponível em: <https://www.economist.com/business/2013/04/06/robot-recruiters>, a IA permitiu à empresa poupar cerca de 266 milhões de euros na retenção de trabalhadores através de fidelização e retenção dos profissionais à empresa ao desenvolver um algoritmo capaz de prever, com um grau de exatidão de cerca de 95%, quais os trabalhadores que ponderam (ou poderão vir a ponderar num futuro próximo) abandonar a empresa, orientando os gestores na melhor estratégia para os reter.

9 Enquanto plataforma de matching de aquisição de talentos, o seu sistema apresentou um tempo de redução do processo de recrutamento das empresas de 75%, e o dobro do rendimento a nível de contratação. Acerca do funcionamento do seu algoritmo patenteado, *vide* Polli, Frida & Yoo, Julie, "Systems and methods for data-driven identification of talent", 2019 e Dencik, Lina, Edwards, Lilian & Sánchez-Monedero, Javier, "What does it mean to 'solve' the problem of discrimination in hiring? Social, technical and legal perspectives from the UK on automated hiring systems", in: Conference on Fairness, Accountability, and Transparency, 2020, pp. 458-468, (p. 462).

10 Cfr. Hirevue, "Bias, AI Ethics, and the HireVue Approach", 2019, disponível em: <https://www.hirevue.com/why-hirevue/ethical-ai>, onde na mesma linha da *Pymetrics*, possibilitou que uma cadeia de hotéis de grande dimensão reduzisse o tempo de contratação de mês e meio para uma semana. Desenvolvendo exemplos comprovados de plataformas neste contexto, *vide* a preciosa análise de Dencik, Lina, et al., op. cit., pp. 458-468. Para uma perspetiva comparada, vide Besse, Philippe, "Détecter, évaluer les risques des impacts discriminatoires des algorithmes d'IA", 2020, disponível em: <https://hal.archives-ouvertes.fr/hal-02616963/document>, pp. 14-15 acerca das principais plataformas de contratação enquanto ferramentas que afastam a existência de discriminação, como a *JobiJoba*, a *Assessfirst*, a *Clémentine*, a *365talents* e a easyrecrue.

definição de perfis[11], favorece a recolha e tratamento dos dados pessoais dos trabalhadores por parte das empresas e instituições permitindo-lhes otimizar as opções e estratégias comerciais e de intervenção, podendo inclusive conferir benesses para as próprias pessoas como é disso exemplo os dados de saúde, mantidos nos hospitais ou nos centros de saúde, cujo acesso rápido facilita o tratamento do doente, quando necessário[12]. *Quarto*, afasta o preconceito e a subjetividade humana substituindo-os por um processo técnico neutro[13] por ser mais objetivo e assertivo, o que possibilita recrutar pessoas da mais variada índole apelando à diversidade do local de trabalho[14], impedindo que certas características humanas tendenciosas, preconceituosas e injustas, como contratar alguém que partilhe dos mesmos gostos do recrutador ou alguém pertencente à mesma *Alma Mater* ou à mesma família que o empregador sejam fatores determinantes[15], daí que a contratação possa servir como apoio a uma maior igualdade no local de trabalho em comparação com os métodos de contratação mais tradicionais. *Quinto*, poderá ser mais minucioso nas análises que faz, na atenção ao pormenor que muitas vezes escapa ao falível olho humano.

Fruto deste cenário idealista e perfeito existe um número razoável de empresas[16] que ao dia de hoje recorre a algoritmos, porém, a verdade é que não

---

11 Que nos termos do número 4 do art. 4º do RGPD é entendido como "qualquer forma de tratamento automatizado de dados pessoais que consista em [utilizá-los] para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações".

12 Na esteira de Palma Ramalho, Maria do Rosário, "A Economia Digital e a Negociação Coletiva", in: CRL, Ministério do Trabalho, Solidariedade e Segurança Social, 2018, pp. 1-165, (p. 65).

13 Cfr. Ajunwa, Ifeoma, "Platforms at Work: Automated Hiring Platforms and Other New Intermediaries in the Organization of Work", in: Work and Labor in the Digital Age, Vol. 33, Emerald Publishing Limited, 2019, pp. 61-91.

14 Cfr. Bornstein, Stephanie, "Antidiscriminatory Algorithms", in: Alabama Law Review, Vol. 70, n.º 2, 2019, pp. 518-572, (pp. 532-533).

15 Desenvolvendo este ponto, *vide* Adelmann, Lena, & Wiedmer, Jennifer, "Der Einsatz von Künstlicher Intelligenz in der Rekrutierung", in: Universität Basel Wirtschaftswissenschaftliche Fakultä, 2020, pp. 1-7, (p. 5) e Teetz, I., "Künstliche Intelligenz im Recruiting", in: Digital HR: Smarte und agile Systeme, Prozesse und Strukturen im Personalmanagement, Petry, T.; Jäger, W. (Hrsg.), Haufe Lexware GmbH, 2018, pp. 225-240.

16 Como os reconhecidos exemplos da *Microsoft, J.P. Morgan, Goldman Sachs, Credit Suisse, Netflix*, entre outros.

estamos perante algo que apresenta soluções mágicas ou infalíveis, até pelo contrário. Deste modo, repudiamos este fenómeno como sendo uma "aura de objetividade e infalibilidade"[17] ou até de *mathwashing*[18], pelo que se afasta a ideia que nos encontramos ante uma espécie de oráculo[19] profético que contém nada mais que a verdade. Inversamente, é necessário não nos deixarmos iludir com a ideia de que os números, *rectius*, os algoritmos não mentem, antes atendendo efetivamente ao conteúdo, à substância que transparece uma realidade bastante diferente e, até certo ponto, assustadora. Aliás, esta ideia de confiança implícita que a maior parte das pessoas deposita no resultado dos algoritmos denomina-se por <<*algorithmic authority*>> na medida em que, a nível social, é conferido um valor superior às decisões que toma, o que muitas vezes dá azo a um certo tipo de culto, como se tratassem de "deuses" cujos comandos devem ser seguidos sem serem questionados[20] e este parece ser precisamente o problema: os algoritmos que estão na base do modelo de negócio de muitas empresas geram injustiças porque se baseiam em modelos matemáticos que reproduzem preconceitos e vieses humanos, o que se repercute na tomada de decisões e na automatização dos processos, i.e., a jusante. Repare-se que não surgem do nada, são criados pelos seres humanos, são ferramentas projetadas por pessoas que têm controlo sobre o seu funcionamento, daí que possam servir, ou para quebrar injustiças e promover a igualdade, ou para perpetuar a exclusão e discriminação ao espelhar o *status quo* do ser humano, o que mais se observa infelizmente na maioria das vezes ainda que provocado de forma não consciente e acidental[21], pois para mal dos nossos pecados a verdade é que não somos agentes económicos racionais, somos tendenciosos por natureza

17 Cfr. Osoba, Osonde A., & Welser IV, William, An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence, RAND Corporation, 2017, pp. 1-29.

18 Como esclarece Joh, Elizabeth E. "Feeding the Machine: Policing, Crime Data, & Algorithms", in: William & Mary Bill of Rights Journal, Vol. 26, Issue 2, 2017, pp. 287-302, (p. 292), pode ser definido como a (errónea) perceção de que modelos algorítmicos não possuem a subjetividade inata ao ser humano, suprimindo-a por se tratar de um sistema matemático.

19 Cfr. Ajunwa, Ifeoma, "The Paradox of automation as anti-bias intervention", in: Cardozo Law Review, Vol. 41, Issue 5, 2020, pp. 1671-1742, (pp. 1688-1690).

20 Cfr. Harari, Yuval Noah, Homo Deus: A Brief History of Tomorrow, Harper, 2017.

21 Não temos dúvidas que a regra geral é depararmo-nos com formas de discriminação não intencionais, em que os empregadores têm o sincero e legitimo interesse em selecionar os melhores candidatos para a vaga disponível, contudo o algoritmo não tem consciência para distinguir o certo do errado.

e intolerantes, de maneiras que não queríamos ser, somos preconceituosos e estamos a injetar esse preconceito no algoritmo.

Um dos principais problemas é, por isso, a tomada de decisões discriminatórias pelo algoritmo que se poderá dever: **(i)** à possibilidade dos algoritmos reproduzirem, de facto, o preconceito humano onde releva a possibilidade de surgimento de novas fontes de discriminação no acesso ao emprego. A este respeito, veja-se as decisões de recrutamento que são por vezes tomadas com base numa variedade de atributos não intuitivos como é exemplo a variável que os cientistas de *data* descobriram ter valor preditivo: a distância do domicílio até ao trabalho[22]. De acordo com esta variável, pessoas com viagens mais longas sofrem maiores taxas de desgaste, porém, a distância pendular está intimamente ligada ao local onde uma pessoa mora que, por sua vez, é conexa com preços da habitação que estão relacionados com a renda e, consequentemente, com a etnia. Deste modo, possibilitar que o algoritmo contrate com base no local onde moram as pessoas – ainda que de forma indireta não intencional - tem provavelmente um impacto adverso em grupos protegidos como as minorias raciais, sendo este um exemplo de um raciocínio algorítmico[23]; **(ii)** à própria construção do algoritmo que requer dados que contêm fatores de discriminação. Com efeito, o algoritmo toma a realidade como fator de aprendizagem na hora de processar dados, o que implica que os resultados extraídos venham a perpetuar discriminação na nossa sociedade, daí que, enquanto não se proceder a uma reforma a nível de coleta do histórico e da definição do sucesso de cada empresa, o argumento de que a máquina é imparcial não passará de uma utopia, pois a verdade é que, o facto dos dados processados serem opiniões do contratante (*in casu*, o empregador) apresentam uma (intensa e clara) componente subjetiva[24], precisamente o inverso da

22 Cfr. Cappelli, Peter, "Your Approach to Hiring Is All Wrong", in: Harvard Business Review, 2019, pp. 48-58.

23 Poderíamos mencionar outros exemplos, como a religião que pode estar estatisticamente relacionada com o código postal da cidade onde a pessoa vive, ou mesmo o tempo dedicado a redes sociais e profissionais - como o *FB* ou o *LinkedIn* – que podem indicar a correspondente afiliação política ou sindical e com isso prejudicar alguém numa determinada decisão. Nesta linha, com outros exemplos semelhantes, *vide* Kullmann, Miriam, "Discriminating Job Applicants Through Algorithmic Decision-Making", in: Ars Aequi, Vol. 68, n.º 1, 2019, pp. 45-53.

24 Miller, Alex P., "Want Less-Biased Decisions? Use Algorithms", in: Harvard,

ideia que querem transmitir i.e., de que são objetivos e justos atuando como profetas da imparcialidade; **(iii)** ao facto de que, quando um algoritmo está no comando, as minorias ficam geralmente em desvantagem devido à falta de informação disponível acerca das mesmas, ou seja, a ideia é de que nas minorias – pertencentes a um qualquer fator discriminatório - haverá menos dados disponíveis, o que implica que o algoritmo entenda que tomar uma decisão favorável a um grupo minoritário seja mais arriscado do que fazê-lo a favor de um grupo maioritário, ou seja, para selecionar um candidato de um grupo minoritário o algoritmo exigirá mais qualidades, habilitações e conhecimento comparativamente a um grupo maioritário simplesmente por ser mais fácil de prever estatisticamente o comportamento de alguém pertencente a este do que àquele grupo[25]; **(iv)** à adoção de regras que, embora aparentem neutralidade, indiretamente revelam discriminação tendo um impacto desproporcional em determinado grupo, *e.g.,* eliminar candidatos que tiveram interrupções superiores a um ano na sua carreira, o que vai prejudicar de forma desproporcional as mulheres que muitas vezes se afastam temporariamente da vida profissional em razão da maternidade.

Assim, os algoritmos condenam-nos a repetir o passado do qual queríamos fugir ao replicarem preconceitos mas com uma capacidade muito superior de discriminação[26], de uma maneira silenciosa e muito menos transparente uma vez que, fruto de questões relacionadas com a programação e design, funcionam

---

Business Review, Vol. 26, 2018, dá-nos uma perspetiva interessante ao alegar que os que tecem críticas à utilidade do algoritmo esquecem-se de responder à questão de saber se, mesmo com as suas debilidades, o desempenho algorítmico se compara ao status quo humano, enunciando alguns estudos suportados por casos reais que auxiliam a conclusão de que os algoritmos são menos tendenciosos e mais precisos em termos comparativos. Pessoalmente, não podemos concordar com esta linha argumentativa uma vez que, no final do dia, o que se revela mais determinante é aferir do balanço a nível da magnitude das consequências perante um cenário negativo, e nesse campo, as inúmeras incertezas aliadas à falta de respostas inequívocas acerca dos problemas relacionados com esta questão tão sensível, leva-nos a não nos comprometer com a adoção pura de um sistema algorítmico dotado de tanto poder, não valendo a pena esse risco.

25 Cfr. Todolí-Signes, Adrian, op. cit., p. 6.

26 Cfr. La Diega, Guido Noto, "Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information", in: JIPITEC, Vol. 9, n.º 1, 2018, pp. 1-33 e Coelho Moreira, Teresa, "Igualdade de género no Trabalho 4.0", in: APODIT 5: A igualdade nas relações de trabalho (coord. Maria do Rosário Palma Ramalho e Teresa Coelho Moreira), AAFDL, Lisboa, 2019, pp. 45-68, (pp. 63-67).

como uma *black box*[27], em que por vezes nem o próprio programador conseguirá aferir do porquê do algoritmo ter chegado a um determinado resultado que se revela controverso, enquanto reflexo da infra informação tecnológica inerente ao homem médio, pois a maioria dos programadores possui um conhecimento muito insuficiente e diminuto acerca das vicissitudes do contexto de emprego o que faz com que criem os seus modelos com parca ou pouca informação útil[28]. Todas estas *red flags*, enquanto fatores de risco, são ainda mais sérios quando tais práticas se baseiam na IA de autoaprendizagem, com o software a ser capaz de reprogramar os seus próprios critérios e métricas para alcançar um resultado predefinido[29] tornando os efeitos nefastos em larga escala.

3. Indícios práticos de vicissitudes no contexto atual: os problemas ético-

27 Como apontam 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 decisões tomadas exclusivamente com base na exploração e prospeção de dados pessoais", in: Fórum de Proteção de Dados, n.º 6, 2019, pp. 60-91, (p. 87), "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", existindo duas configurações comuns de testagem do software: *white box* e *black box*. Nas primeiras, o analista tem acesso ao *source code*, nas segundas, o analista está limitado a observar apenas as entradas (*inputs*) e saídas (*outputs*) do sistema, mas não o seu funcionamento interno (cfr. Desai, Deven R., & Kroll, Joshua A., "Trust but verify: A guide to algorithms and the law", in: Harvard Journal of Law & Technology, Vol. 31, n.º 1, 2017, pp. 1-64, (p. 36). Estamos perante a polémica discussão sobre saber se se deve abrir ou não a Caixa de Pandora que, in casu, significa aceder ou não ao código algorítmico, entrando consequentemente no problema de confronto com outros interesses constitucionalmente protegidos, podendo colocar em causa a segurança, o interesse económico e comercial das empresas e os *IP rights* detidos pelas entidades públicas e privadas, temática que iremos abordar no Cap. III, ponto §2.

28 Quando têm (apenas) em conta, *e.g.*, os melhores desempenhos de trabalhadores no passado de determinada empresa identificando, a partir daí, quais os candidatos a emprego que têm os mesmos atributos, o que provoca discriminação *ab initio* a montante, inquinando todo o processo decisório. Neste sentido, vide Goldenfein, Jake, op.cit., p. 49.

29 Acerca da (não) programação de sistemas inteligentes e as questões laterais que fazem surgir, *vide* Festas, David. "A contratação eletrónica automatizada", in: Direito da Sociedade da Informação – Vol. VI, Coimbra Editora, Coimbra, 2006, pp. 411-461. Nesta linha, Kullmann, Miriam, op. cit., pp. 47-48, distingue entre modelos determinísticos ou modelos de autoaprendizagem "supervisionados" nos quais existe sempre uma decisão consciente (humana) que afeta o algoritmo e um modelo de dados que este utiliza para resolver o problema específico que podem ser ajustados e, por outro lado, os modelos "não supervisionados" que são capazes de se adaptar e determinar por si próprios quais os dados que irão utilizar para o efeito.

-jurídicos das decisões algorítmicas

A questão passa então por saber se, na prática, com os algoritmos, somos capazes de eliminar o preconceito humano ou se simplesmente o camuflamos com a tecnologia a partir do momento em que estamos perante uma intensificação do controlo eletrónico praticamente ilimitado e ainda mais intrusivo para a privacidade, chegando a falar-se em *algocracy*[30] ou <<trabalhador algoritmo>> podendo correr-se o risco de uma coisificação da pessoa humana. Isto leva alguma doutrina[31] a recear pela ausência de liberdade e democracia num futuro próximo sendo este o (infeliz) Estado de Arte dos dias correntes, em que os preocupantes efeitos perniciosos do algoritmo ofuscam as vantagens da implementação de uma sociedade pós-industrial informatizada[32].

3.1. A discriminação

Primo, o primeiro caso real relatado de um algoritmo discriminatório que remonta à década de 1970, em que a Faculdade de Medicina do Hospital de *St. George*, no sul de Londres, recebia mais de doze candidaturas para cada uma das suas 150 vagas anuais. Ora, à data, grandes organizações como o Pentágono, já utilizavam sistemas inteligentes para tratar de candidaturas, mas para um Hospital criar o seu próprio programa de avaliação automatizada no final dos anos 70 representou uma experiência ousada, o que se revelou um fracasso total. *St. George* foi o pioneiro involuntário e inconsciente destas *WMDs* em

30 Ao fim ao cabo, pegando nas palavras de Rota, Anna, "Rapporto di lavoro e big data analytics: profili critici e risposte possibili", in: Labour & Law issues, Vol. 3, n.º 1, 2017, pp. 32-52, (p. 35), assiste-se a um conjunto de dinâmicas cuja força disruptiva alimentada por sistemas computacionais e algorítmicos fomenta a difusão crescente de um novo modelo de governação.

31 Cfr. Tejero, Emilio L., "Algoritmos. El totalitarismo determinista que se avecina. ¿La pérdida final de libertad?", in: Revista de Pensamiento Estratégico y Seguridad CISDE, Vol. 5, n.º 1, 2020, pp. 85-101.

32 Termo utilizado por Coelho Moreira, Teresa, "Algumas notas sobre as novas tecnologias de informação e comunicação e o contrato de teletrabalho subordinado", in: Scientia Ivridica, Vol. 64, n.º 335, 2014, pp. 323-343, (pp. 323-324) para caracterizar esta nova Era de mutação económica radical fruto da inserção das NTIC ao provocar um gradual desaparecimento das fronteiras técnicas que anteriormente permitiam distinguir os diferentes sectores da economia, uma vez que se assiste a uma perda de protagonismo dos sectores primário, secundário e terciário para o setor quaternário da informação.

que os objetivos de eficiência e justiça não foram cumpridos. Tendo o Hospital registos volumosos de candidaturas rejeitadas dos anos anteriores, o trabalho era ensinar ao sistema algorítmico como replicar os mesmos procedimentos que os seres humanos estavam a seguir, sendo que os respetivos *inputs* foram precisamente o problema pois foi através deles que o algoritmo aprendeu como discriminar e realizou esse trabalho de maneira extremamente eficiente na medida em que, para além da discriminação contida no *input* ser racista e xenófoba, um número considerável de candidaturas com nomes ou endereços estrangeiros veio de pessoas que claramente não dominavam o idioma inglês, e em vez de considerar a possibilidade de bons médicos aprenderem a língua, a tendência era simplesmente de os rejeitar automaticamente. De igual modo, interligaram as candidaturas rejeitadas do passado com locais de nascimento e apelidos fazendo com que pessoas oriundas de certos locais, como África, Paquistão ou bairros de imigrantes, recebessem uma pontuação mais baixa sendo, consequentemente, excluídas do processo[33]. Na mesma linha, também se rejeitavam as candidatas com a justificação muito comum à época de que as suas carreiras provavelmente seriam interrompidas pelos deveres da maternidade, e o algoritmo, consequentemente, fez o mesmo juízo. Por todo este conjunto de razões, a Comissão de Igualdade Racial do governo britânico considerou, em 1988, o Hospital culpado de discriminação racial e de género na sua política de admissões[34], estimando a Comissão que, no mínimo, cerca de sessenta dos dois mil candidatos viram, anualmente, uma entrevista ser-lhes rejeitada derivado de um fator de discriminação.

---

33 A este respeito, *vide* o estudo de Banerjee, Rupa, Oreopoulos, Phil, & Reitz, Jeffrey G., "Do Large Employers Treat Racial Minorities More Fairly? A New Analysis of Canadian Field Experiment Data", in: Canadian Public Policy, University of Toronto Press, Vol. 44, n.º 1, 2018, pp. 1-12, cuja investigação demonstrou que, candidatos com nomes chineses, indianos ou paquistaneses tinham cerca de 28% menos probabilidades de obter um convite para uma entrevista de emprego do que os candidatos que tinham nomes com sonoridade inglesa, independentemente de terem as mesmas qualificações. Na mesma linha, vide o interessante estudo de Bertrand, Marianne & Mullainathan, Sendhil, "Are Emily and Greg More Employable than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination", in: American Economic Review Vol. 94, n.º 4, 2004, pp. 991-1013.

34 A nível de consequências do caso, com maior desenvolvimento, *vide* Barocas, Solon & Selbst, Andrew D., "Big Data's Disparate Impact", in: California Law Review, Vol. 104, 2016, pp. 671-732, (p. 682); Garcia, Megan, "Racist in the machine: The disturbing implications of algorithmic bias", in: World Policy Journal, Vol. 33, n.º 4, 2016, pp. 111-117 e O´NEIL, Cathy, op. cit., pp. 115-122.

Secondo, o enigmático caso recente da *Amazon* e do seu algoritmo sexista[35] que, ao replicar as tendências passadas de contratação na empresa excluía as mulheres. Isto sucedia porque os modelos algorítmicos foram treinados para vetar candidatos através da observação de padrões nos *CVs* submetidos à empresa num período temporal de cerca de 10 anos que apontava para um universo de trabalhadores predominantemente do sexo masculino enquanto reflexo do mercado quase monopolizado por este género na indústria tecnológico-digital[36]. Desta forma, o modelo afeto ao recrutamento aprendeu a penalizar currículos que, *e.g.,* continham palavras ou expressões associadas ao sexo feminino, como "capitã de voleibol", e concedeu classificações mais baixas a licenciados de universidades com nomenclaturas femininas como *Maryland University* ou *University of North Carolina*[37], fazendo notar que a ferramenta que pode fazer milagres pelas empresas no momento de identificar talento, pode também ser uma fonte de discriminação para a qual a maioria dos sistemas jurídicos ainda não está preparado para responder. A falta de imparcialidade na abordagem de contratação serviu assim como um *wake up call* ao demonstrar o quão arriscado é para as empresas deixar as decisões de contratação exclusivamente nas mãos da tecnologia.

---

35 A respeito do fator género, é de mencionar o Relatório OIT, "Trabalhar para um futuro melhor", Genebra, 2019, disponível em: <https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-lisbon/documents/publication/wcms_677383.pdf>, pp. 35-36, ao apelar a "uma agenda transformadora e mensurável para a igualdade de género no contexto do futuro do trabalho, [na medida em que] os algoritmos utilizados no preenchimento das vagas de emprego [se têm] revelado perpetuadores de assimetrias de género [podendo reproduzir tendências e preconceitos históricos, pelo que] recomendamos a adoção de medidas específicas para garantir a igualdade de oportunidades (…) nos empregos que serão criados com as novas tecnologias".

36 Aliás, em termos globais, tal disparidade é bem notória na contratação de pessoal para cargos técnicos, tal como apresentado nos dados estatísticos por Dastin, Jeffrey, "Amazon scraps secret AI recruiting tool that showed bias against women", Reuters, 2018, disponível em: <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>, relativamente a cargos exercidos em grandes empresas como a *Microsoft*, a *Google* e a *Apple*.

37 Para maiores desenvolvimentos acerca desta forma de discriminação com origem pura e simplesmente nas expressões recolhidas e interpretadas pela *ML*, *vide* Bolukbasi, Tolga, Chang, Kai-Wei, Kalai, Adam, Saligrama, Venkatesh & Zou, James, "Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings", in: NIPS'16: Proceedings of the 30th International Conference on Neural Information Processing Systems, Barcelona, 2016, pp. 4356-4364.

Terzo, a discriminação de *target ads*[38], i.e., quando a publicidade é direcionada especificamente para determinado público-alvo, deixando outros de fora. Cabe formular uma questão de fundo: quando procuramos emprego online podemos ter a certeza de que estamos a visualizar todas as ofertas disponíveis para as nossas qualificações? Podemos confiar na tecnologia e ter a garantia de que não seremos excluídos de um processo de seleção por algum tipo de discriminação tecnológica invisível a olho nu? A resposta é negativa, todo o ser humano tem um determinado comportamento que leva o algoritmo a mostrar-lhe o que poderá ser relevante subsequentemente a ter sido criado um perfil sobre si, tendo sido uma situação semelhante que levou um grupo de mulheres a interpor, no final de 2019, um processo contra o *FB* no Tribunal Federal de São Francisco nos EUA[39], no qual, alegadamente, nove empresas contratantes discriminavam por género, idade e etnia nas ofertas de emprego divulgadas através da rede social. Essencialmente, discutiu-se a possibilidade que o *FB* conferiu às empresas de publicar estes *targeted ads*, que mesmo não contendo na descrição da oferta qualquer fator discriminatório eram exibidos, por decisão dolosa ou negligente do próprio *FB*, apenas a um determinado perfil de utilizadores, consoante a respetiva etnia, idade ou género, o que se revelou preocupante inclusivamente pela dificuldade probatória, tendo o *FB* eventualmente alterado os termos de serviço e erro na programação dos *target ads*, restringindo a sua utilização e tornando mais transparente o modelo de funcionamento na sequência de um acordo extrajudicial alcançado.

38 Para maior desenvoltura neste campo, *vide* os estudos de BLASS, Joseph, "Algorithmic Advertising Discrimination", in: Northwestern University Law Review, Vol. 114, Issue 2, 2019, pp. 416-468 e de Lambrecht, Anja & Tucker, Catherine, "Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads", in: Management Science, Vol. 65, Issue 7, 2019, pp. 2966-2981, (pp. 2974-2975).

39 U.S. District Court for the Northern District of California, Facebook, Inc. Consumer Privacy User Profile Litigation, n.º 18-md-02843-VC, 13.12.2019. Mas existem outros, *e.g.*, o caso Bradley v. *T-Mobile* US, Inc., n.º 5:17-cv-07232 (N.D. California. Aug. 20, 2018), onde os queixosos alegaram que empresas como a *T-Mobile* e a *Amazon* agiram de modo semelhante ao direcionarem os seus anúncios de emprego para o *FB* de uma forma que exclui os trabalhadores mais velhos.

3.2 A parcialidade e arbitrariedade

Veja-se o curioso caso do algoritmo de avaliação de professores[40]. No Estado de NY (e em grande parte dos Estados norte-americanos[41]), os professores são avaliados pelo denominado *Value-Added Model* (MVA), sendo que a cada professor é dada uma pontuação no final do ano letivo de 0 a 20 pontos consoante – e esta é a pedra de toque – o crescimento previsível da prestação dos alunos. Contudo, este modelo algorítmico revelou-se arbitrário, injusto e cego no que diz respeito a recursos e apelações, tanto que foi intentada uma ação por uma professora da quarta classe no Supremo Tribunal de NY em 2016[42] uma vez que, no ano letivo 2012-2013 tinha recebido uma pontuação de crescimento previsível de 14 em 20 pontos, ou seja, uma classificação designada como "Eficaz", significando que tinha atingido a média do Estado para estudantes semelhantes. Mas no ano letivo seguinte, de 2013-2014, tinha recebido uma pontuação de 1 em 20 pontos, ou seja, uma classificação designada como "Ineficaz", significando que estava muito abaixo da média do Estado para estudantes semelhantes. A autora confirmou com o Departamento de Educação do Estado de NY que nem um recurso administrativo nem um recurso ao Comissário da Educação estavam disponíveis para contestar a pontuação que lhe foi atribuída pelo algoritmo e a essência do seu argumento

40 Para melhor contextualizarmos este importante caso real por se tratar de um dos pioneiros em matéria de caso julgado, salienta-se que o MVA teve a sua origem em 1983 numa altura em que a administração Reagan emitiu um alarme sobre o estado das escolas americanas em que num relatório da National Commission on Excellence in Education, "A Nation at Risk: The Imperative for Educational Reform", 1983, disponível em: <https://edreform.com/wp-content/uploads/2013/02/A_Nation_At_Risk_1983.pdf>, o painel presidencial alertou que existia uma maré crescente de mediocridade nas escolas que ameaçava o próprio futuro como nação e povo, sendo que um dos sinais mais notáveis de fracasso foi o número de classificações em queda nos *SAT's* entre 1963 e 1980, cujo relatório não deixava dúvidas de que os culpados seriam os professores. Nesta linha, *vide* o igualmente curioso caso Houston Federation of Teachers Local 2415, et al. v. Houston Independent School District, Civil Action H-14-1189 (S.D. Tex. 2017). Acerca de outros casos de utilização deste modelo, vide O´Neil, Cathy, op. cit., pp. 135-140 e Toyama Miyagusuku, Jorge e Rodríguez León, Ariana, "Algoritmos laborales: big data e inteligencia artificial", in: Revista Themis, Vol. 75, 2019, pp. 255-266, (p. 262).

41 Atualmente, estima-se que são cerca de 40 Estados segundo O´Neil, Cathy, op. cit., pp. 135-140.

42 State of NY Supreme Court, Sheri G. Lederman v. John B. King, Jr., & Candace H. Shyer, RJI n.º 01-14-ST6183, 2016.

assentava no facto do sistema "castigar" injustamente os professores cujos alunos obtêm de forma consistente classificações substancialmente acima dos padrões do Estado, salientando que, para o ano letivo onde obteve 1 em 20 pontos (de 2013-2014), cerca de 67% dos seus alunos cumpriram ou excederam os padrões da disciplina de Matemática e Inglês que lecionava, sendo que a média do Estado de NY foi de 31%, pelo que ficou estupefacta como seria possível ter recebido esta pontuação. Mais incrédula ficou quando observou que, para o ano letivo anterior os seus alunos pontuaram cerca de 69% para ambas as disciplinas, o que não justificava a descida pontual escandalosa que obteve, sendo aliás elogiada no seio académico pelos seus pares bem como pelos seus discentes, pela qualidade do seu ensino.

Na sua decisão, o Supremo Tribunal de NY decretou que, primariamente, o ónus de estabelecer a existência de um padrão arbitrário da parte do algoritmo recaía sobre a autora em razão de constituir precedente norte-americano[43], acabando por concordar com a mesma de que, de facto, a pontuação que lhe foi atribuída de 1 em 20 pontos foi arbitrária por uma pluralidade de razões[44] sendo de extrema importância para o nosso estudo salientar apenas uma que apresenta, consequentemente, várias ramificações: a existência de uma prova convincente e detalhada da existência de preconceito do modelo algorítmico contra alguns professores em ambos os polos do espectro (com alunos de alto desempenho e com alunos de baixo desempenho), que se traduziu: **(i)** na incapacidade dos estudantes de alto desempenho demonstrarem crescimento semelhante a estudantes de baixo desempenho (i.e., se já estavam no topo das suas habilitações, não conseguiam melhorar, sendo exatamente isto que é exigido por este modelo algorítmico); **(ii)** em toda a oscilação não explicada na pontuação da autora, de um ano letivo para outro, de 14 para 1 em 20 pontos possíveis apesar da presença de alunos com pontuação estatisticamente semelhante nas suas respetivas aulas; **(iii)** principalmente, no facto de ter ficado provado que, segundo o sistema algorítmico de NY, as percentagens de professores que se enquadram em quatro categorias diferentes de pontuação se encontrarem predeterminadas: 7% estarão na categoria "Altamente Eficaz",

43 Cfr. Johnson Elec. Const. Corp. v. NY State Dept. of Transp, 124ª.D.3d1199.1200 (3rd Dept. 2015).

44 Id. 43, pp. 11-12.

77% na categoria "Efetiva", 9% na categoria "Desenvolvimento" e 7% na categoria "Ineficaz", sendo que estas quatro categorias permanecerão intactas de ano para ano, independentemente do desempenho dos alunos ter aumentado ou diminuído drasticamente em relação ao ano precedente, concluindo que o referido modelo algorítmico seria, portanto, irracional.

Porém, existiu um *twist* que nos parece um problema grave que se deveu ao facto de, quando o tribunal teve a oportunidade de colocar um entrave, balizar e estabelecer regras relativamente à discricionariedade e arbitrariedade de um algoritmo (especialmente nos EUA fruto da extrema importância dos precedentes), não o fez. É que apesar de decidir a favor da autora, o tribunal não deixou de realçar o facto de que não possui formação educacional, recursos ou tempo para propor uma alternativa plausível ao modelo algorítmico ou correções sólidas para quaisquer falhas do referido sistema e, como tal, não fez qualquer análise crítica sobre o assunto[45], acabando, aliás, por não apresentar quaisquer outras consequências fruto da decisão que tomou, continuando o algoritmo a vigorar normalmente.

4. As decisões individuais automatizadas no RGPD

O art. 22º RGPD, complementado pelo Considerando (71), consagra o direito à não sujeição a *ADMs* baseadas nos dados pessoais do titular[46] procurando combater a discriminação algorítmica, algo reconhecido como direito fundamental da UE nos termos do n.º 1 do art. 21º CDFUE. Salientamos uma primeira nota: a Lei de Execução manteve-se silente quanto ao assunto não se pronunciando, e uma vez que os regulamentos europeus são atos legislativos dotados de obrigatoriedade em todos os seus elementos, revelam-se como diretamente aplicáveis na ordem interna e, por isso, vinculativos, de acordo com o art. 288º TFUE, pelo que o RGPD desempenhará um papel importante na forte harmonização dos países[47] enquanto único regime *ad*

45 Id. 43, p. 11.

46 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", nos termos do n.º 1 do art. 4º RGPD.

47 Podemos identificar diferentes abordagens legislativas no seio interno dos países acerca das *ADMs* na sequência da entrada em vigor do RGPD nos termos da alínea b) do n.º 2 do

hoc contra decisões algorítmicas. Tendo isto presente, é de realçar que o termo "direito", empregue nesta disposição, não significa que o preceito seja aplicável somente quando ativamente invocado pelo titular dos dados, pelo que entendemos que o preceito estabelece uma verdadeira proibição geral[48] da

art. 22º, que refletem a cultura histórica da temática da proteção de dados de cada ordenamento, cuja intensidade varia de acordo com o uso, maior ou menor, das tecnologias. *Primo*, verifica-se uma abordagem negativa em que o E-M não prevê nenhum caso específico de tomada de decisão automatizada permitida, sendo o caso mais usual e exemplo disso Portugal, Itália, Roménia, Suécia, Dinamarca, Polónia, Finlândia, Chipre, Grécia, República Checa, Estónia, Lituânia, Bulgária, Letónia, Croácia, Luxemburgo, Malta, Lituânia, Eslováquia ou Espanha. *Secondo*, uma abordagem neutra, na qual o E-M implementou algo, mas não propõe nenhuma medida específica adequada para salvaguardar os direitos, liberdades e interesses legítimos da pessoa em causa, como a Alemanha e parcialmente, a Áustria e a Bélgica. *Terzo*, uma abordagem mais procedimental, em que alguns E-M proporcionam salvaguardas específicas que se baseiam principalmente numa descrição dos procedimentos que os responsáveis pelo tratamento de dados devem adotar quando executam *ADM*s sobre indivíduos (*e.g.,* notificação, revisão, etc.) ou algumas formas de avaliação do impacto do algoritmo, sendo disso exemplo o UK, a Irlanda e parcialmente, a Eslovénia. Por fim, temos uma abordagem pró-ativa, na qual alguns E-M propõem novas salvaguardas e mais específicas, como o direito de conhecer os parâmetros de ponderação dos algoritmos, sendo disso exemplo o caso Francês e Húngaro. Reunindo a mais recente das legislações apontadas que comprovam a nossa afirmação, *vide*, por todos, MALGIERI, Gianclaudio, "Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' for Algorithmic Decisions in the EU National Legislations", *in*: *Computer Law & Security Review*, Vol. 35, Issue 5, 2018, pp. 1-40, (pp. 8-10; pp. 28-29 e notas rodapé 42-60).

48 Acolhemos de perto a interpretação preconizada pelo GT29º, "Guidelines on Automated Individual Decisionmaking and Profiling for the purposes of Regulation 2016/679", Adopted on 3 October 2017, last Revised and Adopted on 6 February 2018, disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>, pp. 19-20. Aliás, a sua redação parece deixar entender, de forma implícita, que é esse o objetivo sendo complementada pelo Considerando (71) ao mencionar que, "no entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou [E-M] (…), ou se for necessária para a celebração ou execução de um contrato (…), ou mediante o consentimento explícito do titular". Contudo, não é unanime na doutrina, Hordern, Victoria & Ustaran, Eduardo, "Automated Decision-Making Under the GDPR - A Right for Individuals or A Prohibition for Controllers?", *in*: *Chronicle of Data Protection*, 2017, rejeitam que esta secção deva ser interpretada como uma proibição com o argumento de que se os legisladores da UE pretendessem que esta disposição se tratasse de uma proibição geral, poderiam (e deveriam) ter incluído uma linguagem mais clara neste preceito tendo inversamente utilizado uma linguagem mais ambígua de que "o titular dos dados tem o direito de não ser sujeito a uma decisão", o que não indica se o direito a estar livre deste tipo de decisão se aplica *ex ante* ou *ex post*. De igual modo, é invocado um argumento histórico dado que, em 2016, o texto final do RGPD seguiu a abordagem do Conselho qualificando-a como uma exceção, o que faz desta alteração uma rejeição deliberada da proibição. Nesta linha, Meyer, David, "Did the WP29 Misinterpret the GDPR on Automated Decision-Making?", *in*: *IAPP*, 2017, adiciona um argumento sistemático baseado no facto do art. 22º ser colocado no Cap. III centrado nos

tomada de decisões com base exclusivamente no tratamento automatizado[49] "que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar" (cfr. art. 22º/1) e sem prejuízo das exceções contempladas no RGPD (cfr. art. 22º/2), ou seja, caso não haja nenhuma intervenção humana no processo decisório e, por exemplo, a intervenção humana se limite à aplicação da decisão tomada pela máquina sem qualquer influência sobre o resultado[50], daí que os trabalhadores se encontrem automaticamente protegidos dos

direitos, o que sugere que os legisladores pretenderam que fosse interpretado como um direito que pode ser reivindicado pelas pessoas ao invés de proibir determinadas decisões. Porém, os críticos deste último ponto de vista podem argumentar que existem várias disposições no Cap. III que simultaneamente impõem obrigações aos responsáveis pelo tratamento e concedem direitos às pessoas em causa, como é exemplo disso o art. 12º segundo o qual, "o responsável pelo tratamento tomará as medidas adequadas para fornecer qualquer informação", sendo que os arts. 13º e 14º explicam o que o responsável pelo tratamento "deve" fazer. Para mais, é de relembrar, a par de Pehrsson, Emily, "The Meaning of the GDPR Article 22", *in*: *Stanford-Vienna European Union Law,* Working Paper, n.º 31, 2018, pp. 1-32, (p. 21), que o RGPD se baseou no art. 15º da DPD de 1995 cuja maior diferença assenta nas possibilidades de derrogações ao direito, e embora existissem pequenas variações entre os E-M, foram vários os que interpretaram este art. como uma proibição geral, entre os quais Portugal, apoiando a nossa interpretação.

49 O responsável pelo tratamento não pode eximir-se do disposto no art. 22º fabricando uma intervenção humana, pelo que se uma pessoa acabar por examinar e ponderar outros fatores ao tomar a decisão final, já não se preencherá o preceito. Assim, para que se considere haver uma intervenção humana, o responsável pelo tratamento tem de garantir que qualquer supervisão da decisão seja relevante e não um mero gesto simbólico, daí a restrição do escopo do preceito. Essa supervisão deve ser levada a cabo por alguém com autoridade e competência para alterar a decisão e que, no âmbito da análise, deverá tomar em consideração todos os dados pertinentes. Neste sentido, Floridi, Luciano, Mittelstadt, Brent, & Wachter, Sandra, "Why a Right to Explanation of Automated Decision Making Does Not Exist in the General Data Protection Regulation", *in*: *International Data Privacy Law*, Vol. 7, Issue 2, 2017, pp. 1-47, (p. 34), invocam um argumento histórico de que existiu uma clara intenção dos legisladores de excluir a palavra "predominantemente" e adotar uma interpretação restrita da palavra "exclusivamente" (*solely*). Partilhando desta opinião, *vide* GT29º, *op. cit.*, p. 23, a fim de saber quando é que o nível de intervenção humana é considerado significativo, e também os pareceres do ICO, "Feedback request - profiling and automated decision-making", 2017, disponível em: <https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf> e "Guide to the General Data Protection Regulation", 2018, disponível em: <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>. Contra: Bayamlioglu, Emre, "Transparency of Automated Decisions in the GDPR: An Attempt for systemisation", *in*: *SSRN*, 2018, pp. 1-50, (pp. 41-48), defendendo que aferir acerca do grau de intervenção humana que pode ser permitido não se encontra bem clarificado o que impossibilita de dar uma resposta única.

50 Na esteira de Todolí-Signes, Adrian, *op. cit.*, pp. 7-8, pode adotar-se a abordagem filosófica de que um algoritmo não tem qualquer vontade real, logo, não toma decisões, mas produz resultados, pelo que será sempre um ser humano a tomar (no sentido de aplicar) as decisões.

possíveis efeitos deste tipo de tratamento. Resumidamente, o art. 22.º dispõe o seguinte: (i) em regra, existe uma proibição geral das decisões individuais totalmente automatizadas, incluindo a definição de perfis com efeitos jurídicos ou similarmente significativos[51] (n.º 1); (ii) há exceções a essa regra (n.º 2); (iii) sempre que se aplique uma dessas exceções, devem existir medidas para salvaguardar os direitos e liberdades, assim como os legítimos interesses do titular dos dados (n.º 3); (iv) existe uma espécie de exceção à exceção[52], i.e., o titular pode estar sujeito se tiver dado o seu consentimento explícito[53] ou se

51 Embora o RGPD não defina estes dois conceitos, o GT29º, *op. cit.*, pp. 21-23 entende que o art. 22.º abrange apenas os efeitos com impactos graves, ou seja, os seus efeitos devem ser suficientemente grandes ou relevantes para merecerem atenção. Quer isto dizer que a decisão deve ser suscetível de (i) afetar significativamente as circunstâncias, o comportamento ou as escolhas das pessoas em causa; (ii) ou ter um impacto prolongado ou permanente no titular dos dados; (iii) ou nos casos mais extremos, dar origem a uma exclusão ou discriminação das pessoas, sendo que um dos exemplos dados pelo GT29º é precisamente o de decisões que impeçam o acesso de uma pessoa a uma oportunidade de emprego ou a coloquem em séria desvantagem. Relativamente à situação "que o afete significativamente de forma similar", o Considerando (71) apresenta alguns exemplos típicos, sendo de realçar a expressão, para o que nos interessa, "práticas de recrutamento eletrónico sem qualquer intervenção humana".

52 Neste sentido, Gonçalves, Carlos Jorge, e Pinheiro, Alexandre Sousa, em anotação ao art. 22º RGPD, *in*: *Comentário ao Regulamento Geral de Proteção de Dados* (coord. Alexandre Sousa Pinheiro), Almedina, Coimbra, 2018, pp. 389-390. De igual modo, *vide* a interpretação restrita do GT29º, *op. cit.*, p. 24 quanto às *ADMs* que digam respeito a categorias especiais de dados pessoais invocando o preenchimento cumulativo de determinados pressupostos. Contra esta redação, *vide* Baldini, Davide, "Article 22 GDPR and prohibition of discrimination: An outdated provision?", *in*: *Privacy & GDPR*, 2019, ao defender que o seu elemento literal fica aquém de proteger de forma eficaz o direito à não discriminação uma vez que o simples facto de remover categorias especiais de dados não impediria a ocorrência de discriminação, propondo uma solução que acompanhamos que assenta numa interpretação baseada nos direitos na medida em que esta disposição deve ser interpretada como abrangendo não só os dados que imediatamente revelam pertencer a uma categoria especial (*e.g.,* o país de nascimento, que pode revelar diretamente a origem étnica), mas também os dados que indiretamente revelam essa pertença no contexto do processo de decisão algorítmico. No seguimento desta interpretação mais ampla, este último tipo de dados deve ser excluído ou tratado de forma a diminuir a sua correlação com categorias especiais a fim de evitar qualquer resultado discriminatório, o que parece estar de acordo com a jurisprudência do TJUE que tem sustentado, de forma reiterada, que as disposições de proteção de dados devem ser interpretadas de modo a alcançar a sua (maior) eficácia na defesa dos direitos fundamentais (cfr. TJUE, *Google Spain SL, Google Inc. v. AEPD, Mario Costeja González*, de 13.05.2014, Case C-131/12).

53 Parece suficiente a definição de consentimento prevista no ponto 11) do art. 4º e no Considerando (32), não esquecendo que o silêncio não vale como declaração de vontade segundo o RGPD. Criticando a declaração de consentimento do candidato a emprego enquanto fundamento adequado garante da licitude do tratamento ao abrigo do art. 6º RGPD por parte do responsável pelo recrutamento, *vide* Duarte, Tatiana, em anotação ao art. 88º RGPD, *in*:

o tratamento for necessário por motivos de interesse público de relevo e sejam aplicadas as medidas adequadas, baseadas em tratamentos automatizados (n.º 4). Contudo, o que é certo é que alguma doutrina ainda se encontra desconfiada relativamente à clareza da interpretação do preceito, existindo quem teça severas críticas ao próprio articulado[54].

De destacar ainda o *profiling*[55] que consiste na avaliação dos aspetos pessoais de uma pessoa singular envolvendo algum tipo de apreciação ou juízo

Comentário ao Regulamento Geral de Proteção de Dados (coord. Alexandre Sousa Pinheiro), Almedina, Coimbra, 2018, p. 671, chegando a referir em Pinheiro, Alexandre Sousa, *Privacy e proteção de dados: a construção dogmática do direito à identidade informacional*, AAFDL, Lisboa, 2015, p. 812, que "a sacralização do consentimento constitui uma das ilusões mais correntes na história da proteção de dados [adquirindo] características de puro logro" quando aplicado às NTIC. Nesta linha, acerca das especificidades relativas ao consentimento e à sua relação com as *ADM* e com o *profiling* a partir de uma análise minuciosa interpretativa do RGPD, relacionadas com as orientações do GT29º, úteis relativamente ao candidato a emprego acerca de saber quando e como deve ser usado, *vide* por todos, Bayamlioglu, Emre, *op. cit.*, pp. 33-35 e Dencik, Lina, *et al.*, *op. cit.*, p. 466. Contudo, é de realçar que o Considerando (43) afirma não ser possível aceitar a legalidade do processamento de dados com base no consentimento numa relação em que existe um forte desequilíbrio de poder entre as partes e embora RE se refira especificamente à relação entre as Administrações Públicas e os cidadãos, tal consideração parece ser perfeitamente aplicável à relação de emprego. De facto, nas suas orientações sobre o consentimento, o GT29º, "Guidelines on Consent under Regulation 2016/679", Adopted on 28 November 2017, last Revised and Adopted on 10 April 2018, disponível em: <https://ec.europa.eu/newsroom/article29/items/623051>, p. 8 realça que é difícil que ele seja dado em conformidade com os requisitos, principalmente o que exige a forma livre, pelo que dada a natureza da relação entre empregador e trabalhador, o consentimento dado por este não deve ser entendido como válido enquanto regra geral, devendo apenas ser aceite como tal em circunstâncias excecionais. Sobre esta problemática, de forma bastante esclarecedora, *vide* GT29º, *op. cit.*, e a Deliberação interpretativa CNPD 494/2019, de 3 setembro.

54 Por todos, *vide* a análise de Edwards, Lilian & Veale, Michael, "Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling", *in*: *Computer Law & Security Review*, Vol. 34, Issue 2, 2018, pp. 398-404 ao contraporem os principais argumentos invocados pela doutrina europeia e, da mesma maneira a análise de Hintze, Mike, "Automated Individual Decisions to Disclose Personal Data: Why GDPR Article 22 Should Not Apply", *in*: *SSRN*, 2020, pp. 1-15, (p. 3), para quem esta redação levanta mais questões do que aquelas a que responde, e também, Ferreira, Afonso José, "Profiling e algoritmos autónomos: um verdadeiro direito de não sujeição?", *in*: *Anuário da Proteção de Dados*, (coord. Francisco Pereira Coutinho e Graça Canto Moniz), CEDIS, 2018, pp. 35-43 ao densificar o porquê deste "direito" não ter qualquer utilidade prática na realidade.

55 São três as formas possíveis de o utilizar: (i) definição geral de perfis, (ii) tomada de decisões com base na definição de perfis, e (iii) decisões exclusivamente automatizadas, onde se inclui a definição de perfis como disposto no n.º 1 do art. 22º, sendo que a diferença residirá no nível de intervenção humana consoante determinado caso (cfr. Considerando (30)).

sobre a mesma, cuja aceção inscrita no ponto 4) do art. 4º RGPD utiliza a expressão "qualquer forma de tratamento automatizado" e não um tratamento "exclusivamente" automatizado como no art. 22º podendo implicar algum tipo de intervenção humana, pelo que se revela importante relembrar que existem diferenças entre ambos os regimes[56].

4.1. O direito a obter uma intervenção humana

Recuperando alguns exemplos reais, o que é facto é que empresas como a *Amazon* ou a *Uber* não têm apenas o problema da discriminação na fase de entrada, *ab initio*, sendo de igual modo notória a carência de uma *human in command approach*, i.e., da necessidade da última palavra ser da pessoa e não da máquina na fase final da relação jurídico-laboral. Quanto ao primeiro[57], constatou-se que o algoritmo distribuía tarefas aos trabalhadores, media a sua velocidade e diligência por via de um rastreio das taxas de produtividade[58] e, muito importante, gerava automaticamente avisos ou mesmo despedimentos consoante a qualidade ou produtividade do trabalhador, sem qualquer intervenção dos supervisores. Alguns trabalhadores evitavam deslocar-se à casa de banho - fazendo as necessidades em garrafas de plástico - de modo a manter o seu tempo em paridade com as expectativas e cerca de 55% reportaram sofrer a determinado ponto de depressão. Quanto ao segundo[59], verificou-se que

56 Embora tenham vários pontos de contacto entre si, para um desenvolvimento das disparidades das duas figuras, *vide* os pontos enunciados pelo GT29º, *op. cit.*, *maxime* o âmbito de aplicação de cada um, dado que o regime do art. 22º pode acabar por se sobrepor parcialmente à definição de perfis ou resultar da mesma.

57 De realçar a este respeito um relato inédito do jornalista britânico Bloodworth, James, *Hired: Six Months Undercover in Low-Wage Britain*, Atlantic Books, 2018, que atuou disfarçadamente como um trabalhador no armazém da *Amazon* e como condutor da *Uber*, "desmascarando" e trazendo à discussão as condições em que são prestados os respetivos trabalhos associados ao poderio tecnológico digital.

58 Aliás, o sistema foi mais longe ao rastrear o *time off task* na medida em que, se os trabalhadores fizessem descansos e intervalos prolongados, o sistema gerava avisos automaticamente e, eventualmente, o trabalhador poderia ser despedido (cfr. *id*. 57).

59 *Id*. 58. A este respeito, *vide* a importante investigação levada a cabo por Rosenblat, Alex, *Uberland: How Algorithms Are Rewriting the Rules of Work*, University of California Press, 2018, no qual documentou inúmeras queixas dos motoristas da *Uber* por mau funcionamento da plataforma. Especificamente, pela empresa utilizar um sistema de resposta automática contra incidentes e reclamações de trabalhadores, chamando a atenção para o fraco desempenho algorítmico em responder às questões dos trabalhadores - quando o faz - de forma

uma avaliação mais baixa realizada nestas novas formas de prestar labor tem consequências diretas em termos de manutenção do posto de trabalho[60], em que o algoritmo permite que o condutor aceite a viagem (num curto espaço de 15 segundos) existindo no final uma avaliação através da plataforma cabendo ao sistema automático aferir quais os condutores que poderão ser suspensos ou mesmo convidados a deixar a empresa por não terem aceite um número suficiente de viagens, ou por terem uma pontuação baixa dada pelos utentes.

Face a esta (infeliz) realidade, encontramos algo de essencial no n.º 3 do art. 22º RGPD[61] e complementarmente no Considerando (71), nos termos do qual as "garantias deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana[62], de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão". Deste modo, compete ao responsável pelo tratamento (*in casu*, empregador) colocar à disposição do titular dos dados uma forma simples de exercer esses direitos o que realça a necessidade de transparência quanto ao tratamento na medida em que apenas poderá contestar uma decisão ou manifestar o seu ponto de vista se compreender plenamente como foi tomada e com que fundamento[63], e com isto transmitir-se a ideia

deficiente, desprovidas de lógica, sem nexo, ou não darem efetivamente uma resposta, o que demostra uma total falta de sensibilidade (e de condições) para com os trabalhadores.

60 Pense-se, *e.g.,* no despedimento de um funcionário porque a sua reputação digital foi inferior a 4.6 em 5 "estrelas", como exige a *Uber* (cfr. Barocas, Solon, Hwang, Tim, Levy, Karen, & Rosenblat, Alex, "Discriminating Tastes: Uber's Customer Ratings as Vehicles for Workplace Discrimination", *in*: *Policy and Internet*, Vol. 9, n.º 3, 2017, pp. 256-279, (p. 259)). Trata-se de uma situação abrangida pelo âmbito de aplicação do art. 22º RGPD por consistir numa intervenção não humana.

61 Como observável pelas expressões "designadamente" e "pelo menos" do preceito, as garantias estão mencionadas a título meramente exemplificativo, o que significa que poderão ser adotadas outras.

62 Existem três tipos diferentes de envolvimento humano com IA: *human-in-the-loop*, onde um sistema de IA fornece informação a um humano para que este tome uma decisão (IA → Humano → decisão); *human on-the-loop*, onde um humano supervisiona um sistema de IA que toma uma decisão (IA →Decisão → Humano); *human out-of-the-loop*, onde um sistema de IA toma uma decisão sem qualquer envolvimento humano (IA → Decisão). Pregoamos pela primeira opção. Sobre o assunto, *vide* Goldenfein, Jake, *op. cit.*, p. 48.

63 Neste sentido, *vide* o GT29º, *op. cit.*, p. 16 que vai mais longe ao recomendar que, a fim de tornar essas informações úteis e compreensíveis, devem ser dados exemplos reais dos tipos de repercussões possíveis. Contra: Mittelstadt, Brent, Russel, Chris & Wachter, Sandra, "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR", *in*: *Harvard Journal of Law & Technology*, Vol. 31, n.º 2, 2018, pp. 842-887,

de que se trata de uma das mais importantes salvaguardas explicitamente mencionadas no seio de alguns Estados-Membros (E-M)[64] atuando, em teoria, como uma verdadeira válvula de segurança de forma a impedir decisões arbitrárias, injustas e discriminatórias.

4.2. O direito (de acesso) à informação

Como entende Hildebrandt[65] e, entre nós, Graça Moniz[66], o RGPD "expande as categorias de informação a prestar com o fim de garantir um tratamento equitativo e transparente", assumindo particular importância as informações úteis relativas à lógica subjacente prestadas sobre a existência de *ADMs*[67], conferindo um direito *ex post* ao titular de dados através da interpretação conjunta do disposto nos arts. 13º/2, f), 14º/2, g) e 15º/1, h) auxiliados pelos Considerandos (60) e (63) do RGPD[68], pelo que se exige que os responsáveis pelo tratamento prestem informações específicas e de fácil

(p. 874).

64 Curiosamente, os E-M utilizam redações diferentes quando versam sobre esta salvaguarda. Como aponta Malgieri, Gianclaudio, *op. cit.*, pp. 34-35, a lei alemã utiliza "contestação" (*contest*), enquanto a lei holandesa utiliza "*challenge*", a lei irlandesa utiliza "recurso" (*to appeal*) e a lei britânica utiliza "o direito de solicitar ao controlador que reconsidere a decisão", sendo que todos eles acabam por ser sinónimos com nuances ligeiramente diferentes que provavelmente revelam abordagens distintas adotadas. Na Hungria, o responsável pelo tratamento deve informar o sujeito sobre "os métodos e critérios utilizados no mecanismo de tomada de decisão", contudo, não é claro se a explicação deve ser *ex ante* (baseada na funcionalidade geral do algoritmo) ou *ex post* (baseada na fundamentação da decisão). Paralelamente, no caso francês, como denota Castets-Renard, Céline, "Comment construire une intelligence artificielle responsable et inclusive?", *in*: *Recueil Dalloz*, n.º 4, 2020, pp. 225-230, a lei menciona estes dois elementos: informação *ex ante* sobre as regras gerais e especificas que definem o tratamento de dados e as principais características da implementação *ex post*.

65 Hildebrandt, Mireille, "The new imbroglio - living with machine algorithms", *in*: *The art of ethics in the information society*, Amesterdam University Press, 2016, pp. 55-60.

66 Moniz, Graça Canto, "Direitos do titular dos dados pessoais: o direito à portabilidade", *in*: *Anuário da Proteção de Dados*, (coord. Francisco Pereira Coutinho e Graça Canto Moniz), CEDIS, 2018, pp. 11-34.

67 Em termos da duração da prestação das mesmas, *vide* os n.º 1 e 3 do art. 12º e alíneas a), b) e c) do n.º 3 do art. 14º, a par do Considerando (61).

68 Contra: Pehrsson, Emily, *op. cit.*, p. 27, defendendo que os arts. 13º, 14º, e 15º criam direitos à informação, mas não conferem um direito *ex post* para o titular de dados obter informações sobre uma determinada decisão após o facto, o que parece ser reforçado pelos Considerandos (60) e (63) ao confirmarem (apenas) um direito *ex ante* à lógica e às consequências do tratamento.

acesso sobre tais *ADMs*, nomeadamente os fatores tidos em conta no processo decisório, os critérios e a relevância dos mesmos em termos de consequências previstas para o titular dos dados que não seja uma explicação complexa[69], de modo a cumprir as garantias a que se refere o já mencionado no n.º 3 do art. 22º.

Os preceitos mencionam a expressão "informações úteis relativas à lógica subjacente", o que se revela um ponto fulcral uma vez que a complexidade implícita ao processamento operativo do algoritmo torna difícil de compreender o funcionamento do processo interno da decisão automatizada, atuando como uma *black box*[70] pois à medida que os algoritmos se tornam mais precisos e eficientes, tornam-se também mais complexos e, portanto, mais opacos e resistentes ao escrutínio, sendo apenas possível conhecer os *inputs* e *outputs* do processamento. Todo este secretismo e sofisticação que impede o acesso por parte do homem médio deve-se a motivos de concorrência e inovação, encontrando-se o código algorítmico geralmente protegido por *trade secrets* e *IP rights*[71], pelo que se deve procurar equilibrar e conciliar os interesses entre o atual binómio[72] transparência/*IP rights* aliás, enquanto o Considerando (63) RGPD afirma que os direitos de proteção de dados "não devem afetar (...) o segredo comercial ou a [IP] e, particularmente, o direito de autor que protege o software", o Considerando (35) da Diretiva relativa aos *trade secrets* sublinha, de uma forma radical, que os direitos nela consagrados "não devem afetar os direitos e obrigações estabelecidos na Diretiva 95/46/CE [que

69 Neste sentido, GT29º, *op. cit.*, p. 25.

70 Como refere Barocas, Solon & Selbst, Andrew D., "The Intuitive Appeal of Explainable Machines", *in*: *Fordham Law Review*, Vol. 87, Issue 3, 2018, pp. 1085-1139, (p. 1085), mesmo com conhecimento especializado, a base que está no fundo de uma decisão ainda é muitas vezes inescrutável.

71 É possível qualificar quase todas as informações como *trade secret* e argumentar que a sua divulgação é prejudicial para a vantagem competitiva do seu detentor legal, mas para isso, o algoritmo tem de satisfazer os requisitos cumulativos do art. 2º da *Trade Secret Directive* (EU) 2016/943, de 8 junho 2016, que define amplamente *trade secret* como qualquer informação que não é geralmente conhecida, tem valor comercial derivado deste segredo, e tem sido sujeita a medidas razoáveis para garantir que permaneça em segredo. O objetivo desta Diretiva assenta na proteção contra a aquisição, utilização e divulgação ilegal de segredos comerciais, contudo, como indica Kullmann, Miriam, *op. cit.*, pp. 50-51, nada é regulamentado sobre a situação em que o acesso a um segredo comercial, como um algoritmo, é exigido devido a uma decisão (alegadamente) discriminatória.

72 Ambos são garantidos pela CDFUE, respetivamente, nos art. 8º e no n.º 2 do art. 17º.

precede o RGPD], em particular os direitos dos titulares de dados aos seus dados pessoais". Para mais, o art. 5(d) estipula que é possível uma derrogação à proteção do *trade secret* como forma de "proteger um interesse legítimo reconhecido pela legislação da União ou do E-M", como pode ser o direito de obter uma explicação racional, lógica e clara acerca de determinada decisão[73], tendo sido perante este contexto que o GT29º declarou que a proteção dos *trade secrets* não pode ser uma desculpa para recusar a partilha de informações com os titulares dos dados[74] e, na mesma linha, o EDPS declarou que a proteção dos *trade secrets* não prevalece sobre a proteção dos dados pessoais, devendo haver antes um equilíbrio delicado entre os dois direitos[75], equilíbrio este discutido pelo BGH na decisão SCHUFA, de 28.01.2014[76], tendo-se o tribunal pronunciado a favor de que não havia a necessidade de partilhar o algoritmo, o *source code* do software de cálculo ou outros valores estatísticos relacionados com a fórmula de pontuação, baseando-se na proteção do *trade secret*. Na mesmo linha argumentativa encontra-se a solução francesa, tendo o *Conseil Constitutionnel*[77] decidido que, quando os princípios do funcionamento interno de um algoritmo não possam ser comunicados sem infringir um segredo ou um interesse de *IP*[78], nenhuma decisão individual pode ser tomada com base exclusiva nesse algoritmo, procurando desta forma conciliar por um lado, o

73 Neste sentido, Brkan, Maja, "Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond", *in*: *International Journal of Law and Information Technology*, Vol. 27, Issue 2, 2019, pp. 91-121, (p. 98).

74 Neste sentido, GT29º, *op. cit.*, p. 17 e, na mesma linha, Comandé, Giovanni, & Malgieri, Gianclaudio, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", *in*: *International Data Privacy Law,* Vol. 7, n.º 4, 2017, pp. 243-265, (p. 264).

75 EDPS, "Opinion 7/2015' - Meeting the Challenges of Big Data: A call for transparency, user control, data protection by design and accountability", 2015, disponível em: <https://edps.europa.eu/data-protection/our-work/publications/opinions/meeting-challenges-big-data_en>, pp. 7-10.

76 Bgh, Urteil vom 28.01.2014 - VI ZR 156/13. Embora neste caso o poder de decisão residisse num humano, o que difere do caso das *ADMs*, não deixa de servir como paralelo.

77 Conseil Constitutionnel, du 12.06.2018, n.º 2018-765DC.

78 Sendo que a bitola deve assentar na condição de que, se a descoberta de informação exigir um esforço considerável, é provável que seja considerada como não sendo facilmente acessível, premissa esta explorada por Surblyte, Gintare, "Enhancing TRIPS: Trade Secrets and Reverse Engineering", *in*: *TRIPS plus 20 - From Trade Rules to Market Principles (MPI Studies on Intellectual Property and Competition Law, 25),* Hanns Ullrich, et al. (ed.), Springer, Berlin, 2016, pp. 725-760, (pp. 725-738).

sigilo e a propriedade intelectual e, por outro, a transparência e a atribuição de responsabilidade.

Porém, a verdade é que a opacidade do algoritmo[79] pode facilmente ser uma cobertura para uma nova forma de dissimulação de padrões de discriminação. Por esta razão, doutrinários como Pasquale, embora reconheçam que tais medidas poderiam tornar os algoritmos ineficazes, defendem que o código deve ficar disponível e acessível para escrutínio através de meios regulamentares se necessário, sugerindo ainda a utilização de um auditor independente que possa manter o segredo ao mesmo tempo que serve o interesse público[80]. Tomando a mesma posição relativamente a esta questão da legitimidade de acesso ao código algorítmico, encontramos a jurisprudência inédita do TAR da Lazio, de 22.03.2017[81] que decidiu que um algoritmo é um ato administrativo digital e, por isso, sob o regime do direito fundamental (da liberdade) de informação, os cidadãos têm o direito de aceder ao mesmo[82] esclarecendo que, em princípio, se o direito de acesso (liberdade de informação) e o direito à privacidade (entendida aqui como os *trade secrets*, a *IP* e os direitos de autor) entrarem em conflito, o primeiro prevalecerá. Realçando a argumentação do tribunal, este acabou por concluir que o facto do código estar protegido não

79 Acompanhamos Burrell, Jenna, "How the machine 'thinks': Understanding opacity in machine learning algorithms", *in*: *Big Data & Society*, Vol. 3, n.º 1, 2016, pp. 1-12, que distingue três tipos de opacidade algorítmica: segredo empresarial ou estatal, iliteracia técnica, e a resultante de características de *ML*.

80 A favor: Pasquale, Frank, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Harvard University Press, Londres, 2015, p. 141; Burrell, Jenna, *op. cit.*, p. 4. Contra: PARECER CESE, "Inteligência artificial: antecipar o seu impacto no trabalho para assegurar uma transição justa", de 19.09.2018, disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52018IE1473> e o GT29º, *op. cit.*, p. 25 onde apesar de entender que as informações prestadas devem ser suficientemente completas para permitir ao titular dos dados compreender os motivos da decisão, não considera a divulgação do algoritmo necessária no que respeita às obrigações de transparência mencionadas.

81 TAR Lazio, Chamber III bis, *Gilda vs. MUIR*, de 22.03.2017, n.º 3769/2017. O caso tratava da distribuição de um corpo docente pelas províncias italianas que foi determinada exclusivamente por um algoritmo encomendado a uma empresa privada, onde o requerente procurou exercer o direito de acesso mediante o regime de liberdade de informação.

82 Este entendimento pode hoje ser encontrado na Lei de Procedimentos Administrativos Italiana (arts. 22º a 28º), segundo a qual os cidadãos têm o direito de aceder a documentos administrativos se possuírem um "interesse direto, específico e real, correspondendo a uma situação legalmente protegida e vinculada ao documento que se deseja aceder", citando a alínea a) do n.º 1 do art. 22º desta Lei.

preclude a possibilidade de se abrir esta Caixa de Pandora[83], na medida em que, sem o próprio algoritmo, torna-se extremamente difícil compreender a lógica subjacente à decisão final, servindo este acesso para que o trabalhador seja capaz de fundamentar devidamente a sua reclamação caso a decisão afete os seus direitos ou interesses legítimos. Uma interpretação mais restrita que obstaculize a visualização (*disclosure*) do próprio algoritmo não estaria em conformidade com o direito a um recurso efetivo e a um julgamento justo consagrado na CDFUE e na CEDH. Todavia, o tribunal não deixa de referir algo muito importante: é que uma solicitação de FOIA[84] traz uma grande falha ao regime italiano que é a sua limitação ao setor público, contudo não deixou de mencionar que um dos critérios de maior relevância que permite o acesso será o interesse público da questão apesar da relação poder ser entre privados, tal qual o caso em discussão[85]. Embora seja uma abertura muito significativa,

83 Referiu o tribunal: "Imaginemos o que aconteceria se todos os procedimentos fossem manipulados por algoritmos e as solicitações de liberdade de informação não fossem aplicáveis a documentos algorítmicos [por não terem cariz administrativo], o referido regime ainda existiria nos livros, mas não mais na prática". Tecendo severas críticas acerca desta posição do tribunal, *vide* Tabarrini, Camilla, "Understanding the big mind: Does the GDPR Bridge the Human-Machine Intelligibility Gap?", *in*: *Journal of European Consumer and Market Law,* Vol. 9, Issue 4, 2020, pp. 135-143 ao defender a irrelevância da evidente violação dos direitos de autor uma vez que ter acesso à *source code* para chegar a uma determinada decisão, dificilmente ajudaria os titulares dos dados a exercer o seu direito de a contestar pela sua complexidade inerente que se revela como incompreensível para a pessoa comum. Na mesma linha, encontra-se os organismos europeus na sequência dos estudos do MSI-NET (Committee of experts on internet intermediaries) do CE, "Algorithms and human rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications", DGI (2017)12, 2018, disponível em: <https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html>, Villani Report, "Donner un sens à L´intelligence Artificielle: Pour une stratégie nationale et européenne", 2018, disponível em: <https://www.aiforhumanity.fr> e House Of Lords Report, "AI in the UK: ready, willing and able?", 2018, disponível em: <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>, (especialmente) par. 92 (p. 36) e par. 96-99 (p. 38), ao inviabilizarem uma abordagem de "transparência técnica completa" de todo o algoritmo ou *source code* por enfrentarem inevitavelmente a oposição dos detentores de *IP rights*, comprometendo as escassas hipóteses de uma transparência eficaz. Para uma perspetiva comparada, *vide* Correia, Catarina Camacho, "Inteligência Artificial e Propriedade Intelectual", *in*: *CEDIS Working Papers*, n.º 2, NOVA School of Law, Lisboa, 2021, pp. 1-23, (pp. 8-19).

84 Introduzida em Itália pelo Decreto Legislativo n.º 97 de 2016, é parte integrante do processo de reforma da administração pública definido pela Lei n.º 124, de 7 de agosto de 2015, cujos remédios operam *ex post*, posteriormente à tomada de decisão.

85 O que concordamos, aliás, nem faria sentido restringir a sua divulgação à função

muito dependerá de como a jurisprudência europeia se vier a pronunciar num futuro próximo, na procura de um equilíbrio entre informação e privacidade[86] que para já se revela (quase que) inexistente, não tendo ainda tecido qualquer decisão vinculativa.

Nesta esteira, o RGPD desencadeou um vivo debate em torno da questão de saber se existe um efetivo direito de explicação das *ADMs*[87]. A nosso ver, e reforçando a ideia, revela-se premente que o responsável pelo tratamento encontre formas simples de comunicar ao titular dos dados algum tipo de justificação (*e.g.,* o raciocínio subjacente, ou os critérios aplicados para tomar a decisão) de modo a que seja cognoscível, minimamente clara e compreensível pelo titular dos dados e lhe permita contestar a *ADM* de que foi alvo. Daí que defendamos que a informação significativa sobre a lógica envolvida seria idealmente composta pela informação sobre os dados que serviram de base (*input*) à decisão automatizada, a informação sobre os fatores que influenciaram a decisão, a sua importância e peso, e uma explicação razoável sobre a razão pela qual uma determinada decisão foi tomada, utilizando uma forma compreensível, nunca matemática e complexa[88]. De igual modo, a proteção dos

pública: quereria então dizer que a nível jurídico-laboral, os profissionais (*e.g.,* professores) que ocupam a função pública estariam abrangidos, mas os privados não? Não cremos.

86 Na Itália, o primeiro prevalece, mas *e.g.,* o UK tende a favorecer o segundo, e entre nós, nada é dito a respeito de um cenário de intervenção algorítmica. Para maiores desenvolvimentos acerca desta questão a nível comparado, *vide* La Diega, Guido Noto, *op. cit.*, pp. 1-33.

87 Para uma visão exaustiva das posições doutrinárias existentes sobre esta temática, *vide* Caldas, Gabriela, "O direito à explicação no Regulamento Geral sobre a Proteção de Dados", *in*: *Anuário de Proteção de Dados*, (coord. Francisco Pereira Coutinho, Graça Canto Moniz), CEDIS, 2019, pp. 37-53, (pp. 40-45).

88 Cfr. Brkan, Maja, *op. cit.*, pp. 104-111. Neste sentido, chamamos a atenção para o *draft* de relatório explicativo da Convenção n.º 108 do CE, "For the protection of individuals with regard to automatic processing of personal data", draft explanatory report (da denominada "versão modernizada"), 2016, disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6ec2>, p. 13 (ponto 75.), segundo o qual "os titulares de dados devem ter o direito de conhecer a fundamentação subjacente ao tratamento dos seus dados, incluindo as consequências dessa fundamentação, que tenha resultado em quaisquer conclusões, em especial nos casos que impliquem o recurso a algoritmos para as decisões automatizadas, incluindo a definição de perfis. (…) [D]evem poder conhecer a lógica subjacente ao tratamento dos seus dados resultantes de uma decisão de «sim» ou «não», e não somente as informações relativas à própria decisão, [pois] sem a compreensão destes elementos, não é possível exercer efetivamente outras garantias essenciais, entre as quais o direito de oposição e o direito de reclamação junto de uma autoridade competente". Todavia,

IP rights e dos *trade secrets* não pode privar o titular dos dados do seu direito a ser informado sobre a lógica de uma *ADM*, mas pode justificar a limitação do âmbito da informação, pelo que um nível alto, não técnico, de uma descrição da decisão do algoritmo tem maior probabilidade de ser significativa[89]. No fundo, a prestação deste tipo de informação, a par do acesso aos dados pessoais, são condições indispensáveis para que o seu titular possa exercer os demais direitos apreciando a licitude do tratamento sujeita aos critérios do art. 6º RGPD, sendo por esta mesma razão que estes direitos foram descritos, por parte da doutrina inglesa[90], como o núcleo da proteção de dados pessoais. Um contra-argumento poderia ser o de que a expressão "informação útil relativa à lógica subjacente" pode ser encontrada no Considerando (71), mas não no art. 22º e, não tendo o preâmbulo força jurídica vinculativa, a inserção de um direito de explicação na sua redação poderá ter sido algo propositado e intencional da parte do legislador face à discórdia que já se verificava quanto a este assunto na altura da realização dos trabalhos preparatórios, invocando-se assim um argumento histórico[91]. Porém, em primeiro lugar entendemos que está disposto nos já referidos arts. 13.º ao 15.º RGPD capazes de extrair a *ratio* enunciada[92] e, em segundo lugar, esta aposição numa parte não vinculativa do regulamento, como é o Considerando, tem vindo a ser interpretada pela Comissão, esta sim, como

---

o que é certo é que as opiniões se dividem entre a doutrina. A favor: Comandé, Giovanni, & Malgieri, Gianclaudio, *op. cit.*, pp. 243-265; Hodson, Hal & Powles, Julia, "Google DeepMind and healthcare in an age of algorithms", *in*: *Health and Technology*, Vol. 7, Issue 4, 2017, pp. 351-367. Contra: Edwards, Lilian & Veale, Michael, "Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for", *in*: *Duke Law & Technology Review*, Vol. 16, n.º 1, 2017, pp. 18-64.

89 Acompanhamos de perto Cate, Fred H., Kuner, Christopher, Lynskey, Orla, Millard, Christopher, & Svantesson, Dan Jerker B., "Machine learning with personal data: is data protection law smart enough to meet the challenge?", *in*: *International Data Privacy Law*, Vol. 7, Issue 1, 2017, pp. 1-3 e Araci, Gözde, "A Quest for Fair Balance: Testing the Right of Access against IP Rights and Trade Secrets", *in*: *Munich Intellectual Property Law Center (MIPLC),* Master's Thesis, 2019, pp. 1-70, (pp. 13-16).

90 Cfr. L´Hoiry, Xavier & Norris, Clive, "The honest data protection officer´s guide to enable citizens to exercise their subject axxess rights: lessons from a ten-country European Study", *in*: *International Data Privacy Law*, Vol. 5, Issue 3, 2015, pp. 190-204.

91 Cfr. Floridi, Luciano, *et al., op. cit.*, pp. 41-43 e Mittelstadt, Brent, *et al., op. cit.*, pp. 842-887. Acompanhando este raciocínio, PEHRSSON, Emily, *op. cit.*, pp. 25-26 indica que será muito provável que um tribunal determine que o direito à explicação é aqui fortemente encorajado, mas não exigido.

92 Cfr. Powles, Julia & Selbst, Andrew D., "Meaningful information and the right to explanation", *in*: *International Data Privacy Law*, Vol. 7, Issue 4, 2017, pp. 233-242, (p. 233).

uma "aposição propositadamente deliberada" e, por sua vez, reconhecido o seu papel essencial na interpretação das disposições de um ato da UE[93], pelo que a sua referência ao direito de explicação deve ser usada para interpretar adequadamente o art. 22.º ao refletir o contexto da disposição e a principal finalidade do RGPD, que consiste em aumentar a proteção do titular dos dados pessoais[94].

5. O confronto com a discriminação de decisões individuais automatizadas: em especial, no panorama português.

5.1. O quadro legal no fomento da igualdade e no combate à discriminação

Em Portugal, o uso de algoritmos em contexto laboral ainda não é uma realidade ou, pelo menos, uma realidade transversal a um conjunto alargado de entidades empregadoras. Porém, num contexto internacional e realizando um exercício de prognose futura a curto-médio prazo, importa antecipar os desafios e questões da mais difícil resposta que a utilização de algoritmos poderá colocar, de que são exemplo as práticas discriminatórias que implicam uma série de problemas éticos e colocam em causa as liberdades fundamentais, justificando o enquadramento legal exigente e restrito desta matéria.

No que se refere à recolha e tratamento dos dados pessoais e, por sua

93 É verdade que os Considerandos não podem ser utilizados para uma interpretação *contra legem* das disposições do direito da UE, porém, contar com uma abordagem de interpretação conjunta de várias disposições do RGPD, tal como sugerido acima, e a utilização do Considerando (71) para reforçar a interpretação de apoio à existência do direito à explicação, não conduziria a uma interpretação *contra legem*, pelo contrário, serviria como um meio para resolver ambiguidades resultantes da leitura de disposições relevantes do RGPD, como é reforçado por Brkan, Maja, *op. cit.*, pp. 104-111. Na mesma linha, *vide* Klimas, Tadas & Vaiciukaite, Jurate, "The Law of Recitals in European Community Legislation", *in*: *ILSA Journal of International & Comparative Law*, Vol. 15, 2008, pp. 86-88 ao indicarem que, quando o Considerando for claro, controlará uma disposição operacional ambígua (como poderá ser o exemplo do art. 22º), o que significa que a disposição operacional, no que toca à prestação de informações, será interpretada à luz do Considerando.

94 Nesta linha, o Considerando (58) é claro, ao indicar que o princípio da transparência é "especialmente relevante em situações em que a proliferação de operadores e a complexidade tecnológica das práticas tornam difícil que o titular dos dados saiba e compreenda se, por quem e para que fins os seus dados pessoais estão a ser recolhidos", daí que a complexidade do algoritmo de *ML* não sirva de justificação para que não sejam fornecidas as informações ao titular dos dados.

vez, à igualdade e não discriminação, o regime legal ordinário do Código do Trabalho (CT) deve ser articulado com o RGPD, cujas normas deverão ser interpretadas em consonância com as diretivas e convenções europeias nesta matéria[95], não esquecendo os reconhecidos instrumentos europeus[96] ao constituir direito universal[97]. De forma mais concreta, a nível interno, tendo sempre subjacente uma ideia de dignidade da pessoa humana a Constituição (CRP) consagra uma robusta tutela de direitos de personalidade, fomentando a igualdade de oportunidades no acesso ao emprego e proibindo privilégios e discriminações negativas, ou seja, situações de vantagem infundadas e situações de desvantagem, impondo regras de neutralidade no contexto dos processos de candidatura de acesso ao emprego, nomeadamente quanto aos critérios de seleção dos trabalhadores[98] elencando um conjunto de fatores discriminatórios (cfr. art. 13º CRP), que se espelham no campo específico do Direito Constitucional do Trabalho, daí que a Subsecção III do Título II do nosso CT, i.e., do art. 23º ao art. 32º, se revele bastante completa neste campo, nunca esquecendo que o art. 10º CT estende a aplicação das normas respeitantes aos direitos personalidade, igualdade e não discriminação e segurança e saúde no trabalho à prestação de serviços[99]. Desta forma, para efeitos do nosso estudo, apresentam maior relevo os arts. 23º, 24º/1 e 2, a) e c) *in fine*, 25º, 28º e 30º/1 e

95 De salientar a Diretiva 2000/43/CE de 29 de junho, a Diretiva 2000/78/CE de 27 de novembro, a Diretiva 2005/54/CE de 25 de janeiro e a Diretiva 2006/54/CE de 5 de julho, a Convenção das NU sobre a eliminação de todas as formas de discriminação contra as mulheres, a Convenção para a proteção dos direitos do homem e das liberdades fundamentais, de que Portugal é signatário, e de igual modo, de assinalar a Convenção n.º 111 da OIT que proíbe a discriminação em matéria de emprego e atividade profissional.

96 Designadamente a DUDH, a CDFUE, o PIDCP e PIDESC, a CEDH e o protocolo 12 em anexo à mesma.

97 Porque o problema se coloca em grande escala nos EUA dado ser o país que mais utiliza estes sistemas algorítmicos, o ordenamento apresenta como instrumentos principais de combate à discriminação algorítmica o Título VII da Lei dos Direitos Civis de 1964, que proíbe a discriminação no emprego com base numa característica proibida, e o *Age Discrimination in Employment Act of 1967* que proíbe a discriminação no emprego com base na idade de pessoas com mais de quarenta anos.

98 Cfr. Palma Ramalho, Maria do Rosário, *op. cit.*, p. 50.

99 Quanto ao facto dos trabalhadores por conta própria parecerem excluídos da lei de igualdade de tratamento da UE, *vide* Fredman, Sandra, "Equality Law: Labour Law or an Autonomous Field?", *in*: *The Autonomy of Labour Law*, (Alan Bogg, Cathryn Costello, Acl Davies and Jeremias Prassl (eds.)), Hart Publishing, Oxford, 2015, pp. 257-274, (p. 260), que aborda as consequências destes trabalhadores face a decisões algorítmicas.

2 todos do CT, atribuindo-se ao candidato a emprego e ao trabalhador o direito de controlo dessas informações, interessando aqui o disposto nos arts. 26º/1 e 35º/1 da CRP conexos com os arts. 17º/3 e 4 CT, podendo este último preceito revelar-se importante ao permitir que se extraia dele a obrigatoriedade do titular de dados vir a tomar conhecimento no que respeita às decisões algorítmicas, pelo que pensamos que poderá servir como norma remissiva para essa mesma questão, mesmo sendo a letra da lei limite de interpretação faltando, no entanto, balizá-la devidamente, por isso mesmo entendemos que tal corpo normativo poderá e deverá ser adaptado em face da nova realidade da IA[100] hoje com grande influência na relação laboral, embora naturalmente, ao dia de hoje, este regime legal se imponha às novas tecnologias digitais quando estas sejam utilizadas no contexto de processos de recrutamento e mesmo durante a prestação do labor. Contudo, como refere Palma Ramalho[101], "face ao manancial de informação sobre as pessoas, que é hoje facilmente acessível nas plataformas digitais e que consta de armazenamentos de *Big Data*, na prática poderá ser difícil de garantir que, quando usadas no contexto dos processos de recrutamento, as tecnologias digitais se mantenham dentro dos limites impostos pelo sistema legal", aliás, se um sistema algorítmico se diferencia com base em classes recém-inventadas, poderia permanecer fora do âmbito da lei da não discriminação, dado que tem pouco a dizer sobre as previsões algorítmicas[102]. Por último, fazer menção ao facto dos E-M poderem, por lei ou por convenção coletiva de trabalho (CCT),

100 Em Portugal, o n.º 1 do art. 25º do DL 260/2009, de 25 setembro que regula o regime jurídico do exercício e licenciamento das agências privadas de colocação e das empresas de trabalho temporário, estabelece que "o candidato a emprego tem o direito de ser informado, por escrito, sobre: os métodos e técnicas de recrutamento aos quais se deve submeter e as regras relativas à confidencialidade dos resultados obtidos". Parece-nos que esta espécie de lugar paralelo, pode ser um ponto de partida face ao caminho a seguir face ao atual silêncio da Lei de Execução e, desta forma, colmatava-se ou mitigava-se a assimetria informativa e a ausência de transparência à falta de melhor solução sobre esta nova realidade algorítmica que veio para ficar, cujo CT deverá acompanhar nos próximos tempos de maneira urgente ao suscitarem-se questões sensíveis que carecem de resposta e orientação.

101 Palma Ramalho, Maria do Rosário, *op. cit.*, p. 51.

102 Neste sentido, Borgesius, Frederik J. Zuiderveen, "Strengthening legal protection against discrimination by algorithms and artificial intelligence", *in*: *The International Journal of Human Rights*, Vol. 24, Issue 10, 2020, pp. 1-23, (p. 13). Como refere Kullmann, Miriam, *op. cit.*, p. 53, para além da dificuldade de obter prova, as leis de não discriminação da UE, em combinação com o RGPD, proporcionam ao candidato a emprego poucos mecanismos legais que lhe permita reagir em face de decisões discriminatórias tomadas pelo empregador.

adotar regras mais específicas em relação ao tratamento dos dados pessoais dos trabalhadores no contexto do emprego, e em particular para efeitos do processo de recrutamento e da igualdade e diversidade no local de trabalho, nos termos do art. 88º RGPD.

5.2. Da aferição de accountability

Quem deve ser responsável se um algoritmo tomar uma decisão discriminatória? São muitas as indagações e, ao dia de hoje, poucas respostas e certezas. Este grande desafio de apuramento de responsabilidade surge associado aos elevados níveis de heterogeneidade existente no processo de decisão algorítmica, dificultando o estabelecimento do nexo causal ao respetivo dano de modo a apurar e imputar responsabilidades, daí que este assunto seja referido como "o problema de muitas mãos"[103] por existirem várias camadas na construção de um algoritmo e precisamente porque se baseiam em práticas constantes de inovação e atualização[104], denotando-se, por isso, diferentes entendimentos sobre a matéria.

Num primeiro momento, a responsabilidade terá de ser necessariamente da pessoa, pois só perante ele se poderá reagir devidamente e imputar civilmente responsabilidades pelos atos ou omissões que a máquina causou a terceiros[105],

---

103 Cfr. Doorn, Neelke, Fahlquist, Jessica Nihlén, Royakkers, Lambèr, Van De Poel, Ibo, & Zwart, Sjoerd, "The problem of many hands: Climate change as an exemple", *in*: *Science and Engineering Ethics*, Vol. 18, n.º 1, 2012, pp. 49-67.

104 Neste sentido, Medon, Filipe, & Teffé, Chiara Spadaccini de, "Civil Liability and Regulation of new technologies: issues about the usage of AI in Business decision-making", *in*: *Journal of Institutional Studies*, Vol. 6, n.º 1, 2020, pp. 301-333, (p. 305). Como refere Santos González, María José, "Regulación legal de la robótica y la inteligencia artificial: Retos de futuro", *in*: *Revista Jurídica de la Universidad de León*, n.º 4, 2017, pp. 25-50, (pp. 37-38), quanto mais aumenta a autonomia da IA, mais a responsabilidade é diluída entre os múltiplos atores envolvidos no processo.

105 Cfr. Pires, Thatiane Cristina Fontão, e Silva, Rafael Peteffi da, "A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu", *in*: *Revista Brasileira de Políticas Públicas*, Vol. 7, n.º 3, 2017, pp. 239-255, (pp. 247-248); Toboso Sánchez, Belén, *El impacto disruptivo de la Inteligencia Artificial: Estudio prospectivo sobre su configuración en la sociedad y la categorización de su responsabilidad jurídica*, Trabajo de Fin de Grado, Universitad de Girona 2019, pp. 48-50 e González Martínez, Andrea de los Ángeles, *El Derecho de los robots com inteligência artificial, una nueva disciplina jurídica?*, Trabajo de Fin de Grado, Universidad de La Laguna, 2019, p. 23, embora este último A. não descure a imputação de responsabilidade à máquina num futuro próximo à medida que aumenta a sua autonomia e capacidade de decisão independente

único através do qual é exigível o reparo pelo dano causado, conferindo pretensões indemnizatórias que nunca deverão ficar limitadas no seu tipo ou na extensão dos danos a indemnizar, nem nas formas de compensação à parte lesada[106], assente na pobre justificação de que os danos foram causados por um agente não humano porque em momento algum pode ser atribuída à *ML* a noção de culpa ou de dolo na prática dos seus atos lesivos uma vez que partimos de uma vontade que não foi criada de forma totalmente livre, mas sempre sujeita à sua condição de dependência e vontade de um humano[107]. Porém, a verdade é que recentemente, o Parlamento Europeu propôs a criação de uma nova figura jurídica[108] que assenta num *tertium genus* entre pessoas físicas e legais sugerindo a designação de pessoa eletrónica[109] configurada como um sujeito moral dotado de direitos e obrigações por manter capacidades similares (mas nunca iguais) às das pessoas[110], o que se veio a repercutir no Parecer dirigido à Comissão dos Assuntos Jurídicos da União Europeia que contém recomendações à Comissão

---

da programação humana. Neste mesmo sentido, *vide* a Resolução 2015/2103(INL) do PE, de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre robótica, disponível em: <https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html#title1>, sendo de salientar o ponto AD. e o ponto AF.

106 Neste sentido, *vide* os pontos AF. e 52. da Resolução 2015/2103(INL), *id*. 106.

107 Cfr. Núñez Zorrilla, María del Carmen, "Los nuevos retos de la Unión Europea en la regulación de la responsabilidad civil por los daños causados por la inteligencia artificial", *in*: *Revista Española de Derecho Europeo*, n.º 66, 2018, pp. 9-53, (pp. 9-10).

108 Ponto 59(f) da Resolução 2015/2103(INL), *id*. 106. Apologista desta ideia, *vide* Santos González, María José, *op. cit.*, pp. 37-38 e pp. 40-42, que trata de enumerar as semelhanças entre a IA e uma pessoa jurídica (singular e coletiva), bem como as diferenças que podem contribuir para a formação de uma nova categoria jurídica.

109 Cfr. Bonaldo, Arianna, & Cugini, Gianvirgilio, "Intelligenza artificiale: responsabilità nella progettazione e utilizzo di sistemi: Analisi della tematica e riflessi legali, fiscali ed etici", *in*: *Diritto tributario internazionale e dell'UE*, 2020, pp. 39-44, (pp. 40-41). Todavia, como alerta García-Micó, Tomás Gabriel, "Electronic personhood: a *tertium genus* for smart autonomous surgical robots?", *in*: *Data Science, Machine Intelligence, and Law*, Vol. 1, Algorithmic Governance and Governance of Algorithms, (Ebers M., Cantero Gamito M. (eds.)), Springer, 2021, pp. 87-108, (pp. 87-108), a personalidade não é apenas um pré-requisito para a responsabilidade, mas uma construção jurídica complexa que requer um maior desenvolvimento na medida em que se abre uma janela que será difícil de controlar.

110 Ao que cerca de duas centenas de peritos em IA vieram contestá-la, tendo sido submetida uma carta aberta ao PE (cfr. Open Letter: To the European Comission Artificial Intelligence and Robotics, de 05.04.2018, disponível em: <https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2018/04/RoboticsOpenLetter.pdf)>, referindo-se que deverá ser a defesa do ser humano a estar no centro do debate e não a atribuição de direitos à máquina.

sobre disposições de Direito Civil sobre robótica, de 09.11.2016[111], onde se reconheceu que se deve utilizar processos que assegurem o controlo humano e a reversibilidade das operações pelos sistemas inteligentes e que, atendendo ao seu crescente nível de autonomia, deverá ser acompanhada pela adaptação das regras de responsabilidade no que respeita às consequências associadas às suas ações ou inações. De igual modo, doutrina italiana[112] e francesa[113], fala-nos acerca da necessária complementaridade (no futuro) entre o ser humano e a máquina, propondo que a responsabilidade não seja exclusiva do ser humano, devendo acompanhar-se o progresso científico e tecnológico decisivo para um futuro de novas categorias jurídicas, sugerindo uma responsabilidade mútua quer do humano, quer da *AI*. Tendo esta realidade presente, a par de Vítor Fidalgo[114], entendemos que esta rejeição deverá ser categórica, pois ao contrário do que sucede com o ser humano, qualquer personalidade jurídica fonte de direitos e deveres atribuída à máquina será sempre legal e não inerente a ela, pelo que se as pessoas são o princípio e o fim do Direito, o Direito limita-se a constatar a existência de personalidade jurídica no ser humano, o que já não acontece com as pessoas coletivas ou qualquer outro tipo de entidades em que o Direito imputa subjetivamente situações jurídicas à semelhança das pessoas humanas[115], daí que, mesmo que se denote um nível elevado de autonomia na

111 CEAS, Parecer dirigido à CAJUE que contém recomendações à Comissão sobre disposições de direito civil sobre robótica, de 09.11.2016, disponível em: <https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_PT.html>, ponto 4.

112 Cfr. Casonato, Carlo, "Potenzialità e sfide dell'intelligenza artificiale", *in*: *BioLaw Journal*, n.º 1, 2019, pp. 177-182, (pp. 181-182).

113 Cfr. Soulez, Marie, "Questions juridiques au sujet de l'intelligence artificielle", *in*: *Enjeux numériques - L'intelligence artificielle: un enjeu d'économie et de civilisation?,* n.º 1, 2018, pp. 81-85, (pp. 84-85).

114 Fidalgo, Vítor Palmela, *op. cit.*, pp. 879-900.

115 Esta ideia está presente em NAUCIUS, Mindaugas, "Should fully autonomous artificial intelligence systems be granted legal capacity?", *in*: *Teisės Apžvalga Law Review,* Vol. 17, n.º 1, 2018, pp. 113-132, (pp. 116-122), ao mencionar, e bem, que em contraste com a "pessoa natural", a designação "pessoa jurídica" é utilizada para se referir a uma entidade que não é um ser humano, mas para a qual a sociedade opta por conceder algumas das mesmas proteções e direitos legais que às pessoas naturais, tratando-se, por isso, de uma entidade fictícia criada para realizar determinados atos. Nesta linha, a par de Dyschkant, Alexis, "Legal personhood: how we are getting it wrong", *in*: *University of Illinois Law Review*, Vol. 2015, n.º 5, 2015, pp. 2075-2109, (pp. 2084-2085), poder-se-ia argumentar que associando os sistemas de IA à categorização de "pessoas jurídicas", dependendo do seu desenvolvimento, gozariam de direitos e responsabilidades que poderiam ser atribuídos a outras pessoas jurídicas, mas não teriam direitos e responsabilidades inerentes aos seres humanos.

ML, tal não será sinónimo de liberdade[116], e não sendo livre, nunca poderá ser titular de responsabilidade pelos atos que pratique.

O próximo passo será aferir que pessoa (i.e., quem) deverá responder pelo sucedido. Para um sector doutrinário, a responsabilidade será do empregador[117] sendo que é ele quem determina o *how, when and what* do tratamento de dados mesmo que utilize terceiros para realizar tais tarefas, tendo uma responsabilidade acrescida, designada por *information fiduciary*[118], de verificar e assegurar que as práticas laborais não prejudicam terceiros, a par de ações ou omissões referentes à implementação de medidas que evitem alcançar resultados tendenciosos, arbitrariedades e discriminações, pois são eles quem têm a última palavra decisiva[119]. Para outro sector, a responsabilidade deverá ser atribuída ao programador ou mesmo à entidade que cria e comercializa o algoritmo, uma vez que são os mais capazes (ou mesmo os únicos) de decretar a mudança interna no algoritmo, ou seja, por outras palavras, a ideia é que ao criarem um algoritmo que funciona de uma forma particular, tornam-se

116 Neste sentido, Barbosa, Mafalda Miranda, "Inteligência Artificial, E-PERSONS e Direito: Desafios e perspetivas", *in*: *Revista Jurídica Luso Brasileira*, Vol. 3, n.º 6, 2017, pp. 1475-1503, (p. 1482) e Soulez, Marie, *op. cit.*, pp. 82-83, ao salientarem que a autonomia tecnológica da IA está longe do agir ético dos humanos em que radica o ser pessoa, falhando na relação de cuidado com o outro.

117 Cfr. Calo, Ryan, "Open Robotics", *in*: *Maryland Law Review*, Vol. 70, n.º 3, 2011, pp. 571-613, (pp. 604-605).

118 Conceito originalmente proposto por Balkin, Jack, "Information fiduciaries and the first amendment", *in*: *UC Davis Law Review*, Vol. 49, n.º 4, 2016, pp. 1183-1234, (pp. 1183-1234). Nesta linha, Medon, Filipe, & Teffé, Chiara Spadaccini de, *op. cit.*, pp. 317-325 estabelecem o paralelo com os deveres de cuidado, zelo e diligência que adstringe o administrador em prol de uma empresa, não se podendo afastar a responsabilidade pessoal dos administradores por danos decorrentes de sistemas de IA em razão da *culpa in elegendo* pela escolha da tecnologia a partir do momento em que o administrador delega parte dos processos decisórios da empresa num sistema de *AI*.

119 Cfr. Trindade, Beatriz Santiago, "Two years in: does the GDPR already need updates?: a question brought by algorithmic decision-making", *in*: *Anuário de Proteção de Dados* (coord. Francisco Pereira Coutinho, Graça Canto Moniz), CEDIS, 2020, pp. 79-103, (p. 86, nota rodapé (26)). Nesta linha, pode recorrer-se a teorias da negligência como já entendia Oppenheimer, David Benjamin, "Negligent Discrimination", *in*: *University of Pennsylvania Law Review*, Vol. 141, Issue 3, 1993, pp. 899-972, ao defender que num sistema imprevisível como a proliferação de dados, a maneira correta de pensar sobre a solução poderia passar por um dever de cuidado traduzindo na ideia de responsabilidade sem culpa. Contra este critério, *vide* Santos González, María José, *op. cit.*, p. 39 ao seguir uma orientação assente na responsabilidade de gestão de riscos que não se centre na pessoa que agiu negligentemente, mas na pessoa capaz, em determinadas circunstâncias, de minimizar os riscos e de gerir o impacto negativo.

voluntariamente parte do sistema de decisão e assumem a responsabilidade pelos danos criados, princípios violados e direitos diminuídos do seu sistema de decisão[120]. Para mais, mesmo que o algoritmo aprenda a modificar o próprio código, o facto da intervenção humana ser prévia e a vontade negocial abstrata determinar um afastamento aos princípios clássicos nesta matéria significa que a máquina, por mais sofisticada e complexa que seja, sempre fará aquilo para que foi programada, tendo como fonte a vontade humana, sendo o programador que estabelece os critérios de determinação logo, deve ser-lhe imputada a responsabilidade[121]. Por último, existe um sector que parte da teorização aristotélica[122] de que existem pelo menos duas condições tradicionais para a atribuição de responsabilidade por uma ação, a chamada condição "de controlo" e a condição "epistémica", sendo que uma pessoa é responsável se (i) o fizer (ou o tiver feito) enquanto agente da ação, se tiver causado a ação ou se tiver um grau de controlo suficiente sobre a ação e (ii) se souber e tiver consciência do que está a fazer (ou do que fez). Tendo presente esta orientação filosófica, há quem defenda a repartição de responsabilidades, *maxime* entre o criador, programador do algoritmo e empregador[123] numa espécie de responsabilidade

120 Cfr. Martin, Kirsten, "Ethical Implications and Accountability of Algorithms", *in*: *Journal of Business Ethics*, Vol. 160, n.º 4, 2019, pp. 835-850 e Coeckelbergh, Mark, "Artifcial Intelligence, Responsibility Attribution, and a Relational Justifcation of Explainability", *in*: *Science and Engineering Ethics*, Vol. 26, n.º 4, 2020, pp. 2051-2068, (p. 2059).

121 Neste sentido, de forma mais exaustiva, *vide* Festas, David, *A declaração negocial automatizada*, Relatório de Internet, Direito de Autor e Comércio Eletrónico, FDUL, Lisboa, 2003, pp. 26-41 e pp. 48-72 e, de forma mais sintética, *vide* Festas, David, *op. cit.*, pp. 417-425 e pp. 433-460 ao mencionar que podemos chegar a uma situação de nos encontrarmos fora dos quadros negociais, por impossibilidade de recondução da declaração automatizada à vontade humana (sendo que sem vontade, pode haver imputação e vinculação com aplicação direta ou analógica das disposições do NJ, mas não há NJ), indo mais longe, ao desenvolver a questão acerca da diferença entre os agentes eletrónicos autónomos projetados e os agentes eletrónicos convencionais, na medida em que, o facto dos agentes eletrónicos autónomos projetados poderem aprender com a sua experiência, modificar instruções que lhe tenham sido introduzidas e, no limite, criar instruções próprias, significa que, no extremo, os agentes eletrónicos podem ser programados para se auto-programarem, contudo, a possibilidade de criarem instruções próprias não deixa de resultar da programação originária implementada pelos seus criadores. De igual modo, debruçando-se sobre esta questão, *vide* Medon, Filipe, & Teffé, Chiara Spadaccini de, *op. cit.*, pp. 317-325.

122 Cfr. Aristote, *Éthique de Nicomaque* (trad. Jean Voilquin), Garnier-Flammarion, Paris, 1965.

123 Cfr. Toboso Sánchez, Belén, *El impacto disruptivo de la Inteligencia Artificial: Estudio prospectivo sobre su configuración en la sociedad y la categorización de su responsabilidad jurídica*, Trabajo de Fin de Grado, Universitad de Girona 2019, pp. 48-50

solidária, sendo possível exercer ações de regresso entre as partes responsáveis, posição esta que acompanhamos no seguimento da entrada em vigor do RGPD por via de um critério de finalidade material da recolha e tratamento dos dados pessoais, na medida em que, *e.g.,* numa prestação de serviços de recrutamento e seleção, caso o prestador (exterior) aplique os seus métodos e estratégias de recrutamento com autonomia técnica em relação ao cliente (empregador), i.e., se não receber quaisquer instruções quanto aos métodos e técnicas de recrutamento, exceto quanto ao perfil de candidato a selecionar, não poderá ser entendido como subcontratante no âmbito do tratamento de dados pessoais, mas sim como responsável pelo tratamento (cfr. arts. 28º/3, a) e 29º ambos do RGPD). Para mais, caso o cliente (empregador) determine um perfil de candidato e posteriormente venha a escolher os candidatos a contratar, entende-se que este define as finalidades do tratamento, sendo, por isso, também responsável pelo tratamento. Neste exemplo, o enquadramento da responsabilidade da empresa de recrutamento no âmbito do art. 28º RGPD como subcontratante não se afigura adequado, pois nenhuma das entidades se limita a tratar dados pessoais por conta da contraparte[124], ora se as partes tratam dados em momentos distintos do processo de recrutamento, faz sentido que as

---

e Gordillo Rodríguez, Cristhian Fabián, *La responsabilidad civil en el derecho privado colombiano de la robótica con inteligencia artificial*, Trabajo de Fin de Grado, Fundación Universitaria Los Libertadores, 2020, p. 81. Como apontam King, Allan G., & Mrkonich, Marko, "Big Data and the Risk of Employment Discrimination", *in*: *Oklahoma Law Review*, Vol. 68, n.º 3, 2016, pp. 554-584, (p. 583), apesar do empregador que subscreve a *Big Data* ser responsável pelas consequências mesmo que da sua parte exista falta de intenção ou conhecimento discriminatório do algoritmo, é provável que o seu criador tenha uma perceção mais precisa do risco, uma vez que desenvolveu o produto. Chegando à mesma conclusão pelo caminho da responsabilidade por produtos defeituosos através do regime nacional (*in casu*, Espanhol) de adaptação da Diretiva 85/374, de 25 julho, *vide* Santos González, María José, *op. cit.*, pp. 43-46; Ramón Fernández, Francisca, "Robótica, inteligencia artificial y seguridad: ¿Cómo encajar la responsabilidad civil?", *in*: *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, n.º 9365, Wolters Kluwer, 2019, pp. 1-13, (pp. 7-8) e García-Micó, Tomás Gabriel e Gómez Liguerre, Carlos, "Responsabilidad por daños causados por la Inteligencia Artificial y otras tecnologías emergentes", *in*: *InDret*, Vol. 1, 2020, pp. 501-511, propugnando que a origem do defeito pode estar no fabrico, conceção ou informação sobre o consumo, utilização ou manuseamento do produto fazendo o paralelo para o algoritmo.

124 Atente-se o n.º 10 deste preceito, segundo o qual, "(…) o subcontratante que, em violação do presente regulamento, determinar as finalidades e os meios de tratamento, é considerado responsável pelo tratamento (…) em questão", em conjugação com a definição de responsável pelo tratamento prevista no n.º 7 do art. 4º RGPD.

suas obrigações e responsabilidades sejam repartidas em função da influência no tratamento em determinada ocasião, de maneira proporcional, sendo que o próprio art. 26º RGPD pretende evitar que a diluição da *accountability* pelo tratamento impeça a sua imputação pelo incumprimento dos seus princípios e normas, entendimento que encontra apoio na jurisprudência europeia[125].

Por fim, questiona-se com frequência se seria necessário criar normas e institutos específicos para tratar de matérias atuais relativas à IA ou se deveriam ser aplicadas as normas já existentes, i.e., saber se os regimes de responsabilidade civil atuais seriam suficientemente maleáveis para lidar com os novos conflitos resultantes da relação entre o ser humano e a IA. Seguindo de perto a Resolução 2015/2103(INL), entendemos que o (futuro) instrumento legislativo deverá basear-se numa avaliação aprofundada da Comissão que determine se a abordagem a aplicar deve ser a da responsabilidade civil aquiliana por factos ilícitos ou a da gestão de riscos, consoante exista ou não culpa, dado que esta última modalidade prescinde do elemento subjetivo e tendo em mente que aquele instrumento incentiva – e bem - a adoção de uma responsabilidade objetiva ao ter a benesse de se exigir "apenas" a prova de que o dano ocorreu e o estabelecimento de um nexo de causalidade entre o funcionamento prejudicial e os danos sofridos pela parte lesada[126] sendo que o regime de gestão do risco é dirigido à pessoa capaz de minimizar o respetivo risco e de gerir o seu impacto. Nesta esteira, poderá fazer sentido propor-se o paralelo com a responsabilidade de danos causados por animais (cfr. art. 502º do Código Civil - CC) na linha da teoria do risco, no sentido de que, quem for responsável pelo algoritmo,

---

125 Veja-se o Ac. TJUE, *Jehovan todistajat - uskonnollinen yhdyskunta*, de 10.07.2018, Case C-25/17, ponto 65. e 66.: "Os referidos intervenientes podem estar envolvidos em diferentes fases [do] tratamento e em diferentes graus, pelo que, a responsabilidade das partes deverá ser proporcional ao nível de intervenção no tratamento de dados (…). Uma pessoa singular ou coletiva que, para fins que lhe são próprios, influencia o tratamento de dados pessoais e contribui assim para a determinação da finalidade e dos meios do tratamento pode ser considerada responsável pelo tratamento". Nesta linha, chama-se a atenção para o ponto 56. da Resolução 2015/2103(INL), *id*. 106.

126 Ponto 53. e 54, *id*. 106. Fazendo um apanhado das restantes pronúncias europeias sem, contudo, resultar das mesmas alguma proposta ou clarificação acerca do tipo de responsabilidade que pode estar em causa, *vide* Júnior, José Luiz de Moura Faleiros, "Discriminação por algoritmos de Inteligência Artificial: A responsabilidade civil, os vieses e o exemplo das tecnologias baseadas em luminância", *in*: *Revista de Direito da Responsabilidade*, Ano 2, 2020, pp. 1007-1043, (pp. 1034-1039).

suporta o risco pelos danos que eventualmente venha a provocar tendo que lidar com o perigo decorrente da sua imprevisibilidade[127], isto porque, como vimos, muitas das vezes o fundamento da responsabilidade não assenta num ato culposo, devendo, por isso, ter o seu alicerce no controle de um risco, ou talvez, com maior rigor, no controle de potenciais danos aliado ao princípio da justiça distributiva, segundo a qual quem tiver o lucro ou, em todo o caso, o beneficio de uma certa coisa (*in casu*, de um algoritmo decisório), deve suportar os correspondentes encargos (*ubi commodum ibi incommodum*) apesar da nossa restrita solução legislativa que acolhe, como regra, a responsabilidade por factos ilícitos com base na culpa, uma vez que só existe a obrigação de indemnizar independentemente da mesma nos casos especificados na lei (cfr. n.º 2 do art. 483º CC). Não obstante, é ainda merecida uma menção honrosa à ideia defendida por alguns de imputar responsabilidades de acordo com a decorrente de produtos defeituosos em paralelo com o que é aplicado aos veículos autónomos[128], também ela se mantendo na alçada da responsabilidade objetiva e beneficiando das características presentes no velhinho e ainda em vigor DL n.º 131/2001, de 24 abril (na sua versão mais recente e atualizada) que transpôs a Diretiva n.º 1999/34/CE, de 10 maio, sendo de realçar o facto de ter um conceito amplo de produtor e de produto, a par de uma eventual responsabilidade solidária, ainda que a aplicação deste regime contenha algumas lacunas que nos retraem e impede que esta seja a melhor opção face às idiossincrasias do nosso caso concreto, desde logo, a dificuldade de ligar o empregador a este tipo de responsabilidade.

5.3. Da reação perante a discriminação

Premente na discussão sobre as questões aqui em análise consiste

127 Cfr. Medon, Filipe, & Teffé, Chiara Spadaccini de, *op. cit.*, pp. 317-325.

128 *Id*. 124 *in fine*. Para uma explicação do regime invocado e de um possível paralelo, *vide*, entre nós, Coelho, Vera Lúcia Paiva, "Responsabilidade do produtor por produtos defeituosos. Teste de resistência ao DL n.º 383/89, de 6 de novembro, à luz da jurisprudência recente, 25 anos volvidos sobre a sua entrada em vigor", *in*: *Revista Eletrónica de Direito*, n.º 2, CIJE, Porto, 2017, pp. 1-53 e Silva, Gonçalo Viana da, "Veículos autónomos: um novo desafio para o direito português", *in*: *Data Venia – Revista Jurídica Digital*, Ano 8, n.º 11, s/l, 2020, pp. 5-98.

em saber como proceder[129] diante de uma efetiva discriminação algorítmica direta[130] ou indireta[131], o que contestar e contra quem, perante a existência de uma aparente prova diabólica que deriva do facto de nem o RGPD, nem a própria lei de execução conterem qualquer orientação relativamente ao direito de contestar *ADMs* e ao tipo e grau de envolvimento humano necessário para tal, dificuldade probatória esta que já se revela um problema quanto mais neste contexto algorítmico[132].

Estas vicissitudes são transpostas para o trabalho tradicional, mas também para as novas formas de prestar labor que decorrem das novas tecnologias de informação e comunicação (NTIC), como sucede no interessante caso das plataformas digitais. Tomando como exemplo a *Uber* na qual o algoritmo possui o poder imenso (de entre vários) de despedir trabalhadores consoante o *rating* dado pelos utilizadores, o problema assenta na eventual *score* que não é objetiva, i.e., podemos estar a falar do melhor condutor, amável, preocupado com o bem-estar dos seus clientes e dotado de habilidades ímpares de condução, mas que por ser de determinada nacionalidade, etnia ou género recebe baixas pontuações reiteradas, fazendo com que seja automaticamente

---

129 Recorde-se que o direito de ação também é conferido à associação sindical que represente o trabalhador (cfr. n.º 1 do art. 5º CPT). Para mais, o art. 80º RGPD concede ao titular o direito de mandatar uma entidade não lucrativa, organização ou associação para apresentar uma reclamação ou exercer um direito de proteção de dados em seu nome, o que significa que qualquer sindicato pode, em nome dos seus membros, exercer um direito de acesso, retificação, eliminação ou oposição (entre outros) não só em tribunal, mas também perante o empregador ou uma agência nacional de proteção de dados.

130 Seguimos a definição da alínea a) do n.º 1 do art. 23º CT, semelhante à anglo-saxónica *disparate treatment*.

131 Seguimos a definição da alínea b) do n.º 1 do art. 23º CT, semelhante à anglo-saxónica *disparate impact*. Por levantar mais problemas que a sua congénere, é relevante deixar a nota de que, aqui não é relevante o *animus* discriminatório, sendo antes o efeito de determinada conduta que deve relevar (cfr. TEDH, *Biao v. Denmark*, de 24.05.2016, application n.º 38590/10, par. 91, 92 e 103) ao visar disposições, critérios ou práticas que parecem ser neutras, mas que, de facto, discriminam, podendo ser o exemplo das situações já mencionadas em que os processos de *ML* utilizam dados que incorporam preconceitos do passado, levando assim a resultados imprecisos e não fiáveis. Sobre o assunto, *vide* Kamarinou, Dimitra, Millard, Christopher & Singh, Jatinder, "Machine Learning with Personal Data", *in*: *Queen Mary School of Law Legal Studies*, Research Paper n.º 247, 2016, pp. 1-23, (p. 16), acerca da implementação desta lógica face a indivíduos pertencentes a grupos minoritários.

132 Cfr. Kajtár, Edit e Mestre, Bruno, "Redes sociais e o direito à privacidade dos trabalhadores na fase pré-contratual: algumas questões e considerações comparativas", *in*: *Prontuário de Direito do Trabalho,* CEJ, n.º 2, 2016, pp. 219-243, (pp. 220-221).

desativado da plataforma. Dito isto, como é que se poderá provar o impacto discriminatório do sistema de classificação atribuído? É que as classificações são intencionalmente subjetivas e visam captar o nível geral de satisfação de um cliente com o serviço prestado, mas devido ao seu cariz arbitrário e pessoal, torna-se complicado aferir das efetivas razões que levaram os utentes a atribuir uma classificação considerada fraca (i.e., abaixo de 4.6 "estrelas"[133]), crucial em termos de manutenção do posto de trabalho. Nos EUA, o Supremo Tribunal mantém um precedente importante em *Griggs v. Duke Power Co.,* 401 U.S. 424 (1971) observando que *"[t]he touchstone is business necessity. If an employer practice (...) cannot be shown to be related to job performance, the practice is prohibited"*, cujo *standart* é de tal forma amplo que concede ao empregador uma fácil escapatória e uma justificação suficiente e simples, possibilitando que a *Uber* recuse reter condutores sujeitos a avaliação discriminatória por integrar o sistema classificatório que lhe permite gerir uma grande população geograficamente distribuída e transitória de milhares de trabalhadores em todo o mundo, e muitas alternativas menos discriminatórias levariam à imposição de custos significativos suportados pela *Uber* fruto de uma eventual alteração do sistema que prevê o critério de decisão algorítmico[134], o que por sua vez impediria a empresa de fornecer o seu serviço principal, sendo incapaz de realizar o seu objetivo comercial ao utilizar um sistema de avaliação alternativo.

Face a esta realidade, defendemos a abolição de um critério assente em necessidades empresariais que se revela demasiado amplo, discricionário e facilmente atingível, desequilibrando uma balança que por defeito se revela deficitária e, *ipso facto*, pouco eficiente para o problema sensível que representa, sendo ao invés necessária uma maior objetividade materialmente mais acessível à parte precária, munindo-a dos meios próprios de modo a que consiga atingir o seu propósito ou no limite, que lhe dê essa oportunidade. Para tal, plataformas como a *Uber* poderiam recolher dados sobre as características demográficas dos condutores e associá-las às classificações que são atribuídas, incluindo informação acerca do nível de probabilidade que determinados condutores têm de receber classificações baixas comparativamente a outros e,

133 Cfr. Barocas, Solon, *et al., op. cit.*, p. 259.
134 *Id*. 134, pp. 268-269.

consequentemente de receberem avisos de potencial desativação da plataforma. Mais: deve exigir-se uma mínima justificação dos clientes acompanhada de determinada classificação, principalmente para as mais baixas, *e.g.,* se se deveu a questões relacionadas com a condução, personalidade ou higiene, permitindo fornecer orientações específicas ao condutor e mesmo à plataforma de modo a aferir da veracidade destes dados mais objetivos, o que poderia levar a uma mudança concreta no comportamento do condutor e/ou a demonstrar ao seu superior que a respetiva fundamentação se mostra infundada, não justificando o seu despedimento, sendo indicadores como estes que podem servir melhor os interesses dos trabalhadores de plataforma ao facilitar a identificação de padrões problemáticos no decurso da atividade e permitindo uma efetiva defesa da sua parte. Por fim, deverá repensar-se no critério de tomada de decisão acerca de algo tão sensível como é o despedimento, podendo as classificações atribuídas ser um fator a considerar para esse apuramento juntamente com outras técnicas de avaliação não devendo recair puramente sobre aquelas, toda a decisão[135].

Perante o cenário português que contraria a regra geral no direito probatório de que quem alega um facto constitutivo de um direito que invoca deve prová-lo, em matéria de proteção e promoção da igualdade e não discriminação em sede laboral o legislador teve a noção da dificuldade existente neste campo, pelo que veio a consagrar mecanismos com vista à "inversão" do ónus da prova tendo por base o contributo europeu[136]. Assim, nos termos do n.º 5 do art. 25º CT, o demandante tem o ónus de alegação e o empregador o ónus da prova, contudo, continua a não facilitar a tarefa da parte vulnerável uma vez que tem o ónus de demonstrar que é membro de uma classe protegida e que sofreu um tratamento prejudicial fruto da decisão algorítmica que teve um impacto díspar nas respetivas características protegidas, competindo-lhe

135 *Id*. 134, pp. 271-273.

136 Chamamos a atenção para as Diretivas Europeias (mais recentes) sobre a matéria do combate à discriminação, sendo de realçar o n.º 1 do art. 8º Diretiva 2000/43/CE, de 29 de junho, e o n.º 1 do art. 10º Diretiva 2000/78/CE, de 27 de Novembro, ao estabelecerem que "os E-M tomarão medidas necessárias para assegurar que incumba à parte demandada provar que não houve violação do principio da igualdade de tratamento, cabendo ao demandante apresentar, perante o tribunal ou outra instância competente, elementos de facto constitutivos da presunção de discriminação direta ou indireta". Destes enunciados há quem extraia a conclusão de que não se trata de uma inversão do ónus da prova, mas sim de aligeirar o ónus da prova a cargo do autor. Porém, nos respetivos preâmbulos, apesar do seu contributo tender

a prova do dano sofrido e pelo qual pretende ser indemnizado, situação em que opera a regra geral do n.º 1 do art. 342º CC porque constitutiva do direito, portanto, uma tarefa quase impossível sem acesso aos dados e ao *source code* do algoritmo. Assim, esta alegada "inversão", ainda que louvável, não resolve as dificuldades do demandante, pelo que preferimos a qualificação de repartição do ónus da prova[137], pois apesar de não lhe competir provar que foi efetivamente discriminado, sendo antes da competência da parte passiva (empregador) que trará para a demanda um conjunto de factos dos quais se possa concluir que uma determinada decisão não é realizada com intuitos discriminatórios antes assentando em dados objetivamente fundados que terá de fazer prova de estarmos ante uma presunção de discriminação, a verdade é que consegue facilmente refutá-la ao demonstrar que a decisão está relacionada com a própria atividade profissional e se revela consistente com a necessidade empresarial (*business necessity*)[138], não obstante o queixoso ainda poder demostrar que existe uma alternativa menos discriminatória que o empregador não adotou, portanto, queremos com isto evitar que o n.º 5 do art. 25º CT, quando confrontado com questões de prova referentes à nova realidade da IA nomeadamente de algoritmos discriminatórios, se transforme num preceito meramente simbólico, dotado de um vazio de conteúdo. Exemplificando, se um

---

para a conotação meramente interpretativa não vinculativa, partem do pressuposto de uma verdadeira presunção de discriminação, conforme se extrai dos respetivos Considerandos (21) e (31), nos quais se declara que se impõe a adaptação das regras do ónus da prova em caso de presumível discriminação com a correspondente exigência de que o mesmo incumba à parte demandada, o que leva Fialho, Manuela Bento, "Igualdade no trabalho. Um caminho aberto, uma estrada por pavimentar...", *in*: *Prontuário de Direito do Trabalho*, n.º 76-78 (número especial em homenagem à obra do Dr. Vítor Ribeiro), CEJ, 2007, pp. 91-103 a entender que toda esta formulação legal não deixa dúvidas de que se está perante uma verdadeira inversão do ónus da prova e não apenas de uma maior facilitação do mesmo. No direito comparado também se exige esta solução, *vide* Kim, Pauline T., "Big Data and Artificial Intelligence: New Challenges for Workplace Equality", *in*: *University of Louisville Law Review*, Vol. 57, Issue 2, 2019, pp. 312-328, (p. 324), que pregoa pela existência de uma inversão do ónus da prova e, por sua vez, de uma presunção *iuris tantum* de culpa do empregador. Na mesma linha, *vide* a fundamentação de Ajunwa, Ifeoma, *op. cit.*, pp. 1726-1734.

137 Acompanhamos de perto Carvalho, Paulo Morgado de, "Ónus da prova em caso de discriminação", *in*: *Estudos dedicados ao Professor Doutor Bernardo da Gama Lobo Xavier,* Vol. 3, Lisboa, 2015, pp. 109-136, (pp. 119-122) e Palma Ramalho, Maria do Rosário, *Tratado de Direito do Trabalho: Parte II - Situações Laborais Individuais*, 7ª edição revista e atualizada, Almedina, Coimbra, 2019, pp. 180-181.

138 Porque a verdade é que temos de prevenir o que sucede, de forma muito usual nos EUA como relatado por Barocas, Solon, *et al., op. cit.*, pp. 256-279 de que se uma empresa

candidato a emprego se considerar discriminado diretamente por determinado fator de discriminação terá que alegar qual a decisão que lhe foi imposta (*in casu*, de não o recrutar) e que o foi em função e devido a esse fator, indicando outro(s) candidato(s) a emprego relativamente aos quais tal medida não logrou. Já o empregador terá que alegar e provar que a decisão que impôs àquele candidato encontrava justificação em determinada circunstância[139], sendo neste pormenor que, mantendo-se silente a Lei de Execução, parece compactuar, *mutatis mutandis*, com a solução americana de que a sua justificação tende a prevalecer ao se invocarem *business necessities*, *e.g.,* alegando que o candidato não tem qualidades suficientes ou adequadas às necessidades da empresa após avaliação do *CV*. O mesmo se diga para as situações de discriminação indireta, cabendo, *e.g.,* ao candidato alegar a prática implementada e que essa prática coloca o grupo onde está inserido numa posição de desvantagem através de um exercício comparativo, do outro lado, resta ao demandado alegar e provar que a prática se alicerça em determinado fim legitimo e que os meios para alcançar tal fim são adequados e necessários. Ora, o empregador deve suportar o ónus de demonstrar que o modelo é estatisticamente válido e substantivamente significativo, em oposição a meramente relacionado com o trabalho *e.g.,* que foi construído utilizando dados que são precisos, imparciais e representativos permitindo um melhor contraditório, o que apenas será possível com uma certa abertura do *source code* algorítmico de modo a que o trabalhador seja capaz de rebater o que foi dito e apoiar-se em algo palpável ao fundamentar a sua contestação, pois se não se compreende os processos no *engine room* não será possível identificar violações da privacidade, as causalidades subjacentes e, *ipso facto*, a culpabilidade. Daí a necessidade de distribuir o ónus da prova de

decide quem contratar por via de um algoritmo que se revela claramente preconceituoso mas bem sucedido em prever (o tal "valor preditivo") o desempenho do trabalhador, isso contaria como necessidade empresarial e iria enquadrar-se no argumento de resguardar os interesses da empresa e não como discriminação, sendo assim entendido que uma prática que tem efeito discriminatório é justificada por estar diretamente relacionada com o desempenho no trabalho. Noutras palavras, a lei existente em alguns países parece "apoiar" o uso de algoritmos preconceituosos. Utilizando outros exemplos recorrendo aos principais fatores de discriminação, *vide* Kleinberg, Jon, Ludwig, Jens, Mullainathan, Sendhil & Sunstein, Cass R., "Discrimination in the Age of Algorithms", *in*: *Journal of Legal Analysis,* Vol. 10, 2018, pp. 113-174, (pp. 142-143).

139 Neste sentido, *vide* o Ac. STJ de 20.06.2018, processo n.º 31947/15.9T8LSB.L2.S1, (António Leones Dantas).

uma forma que possibilite efetivamente a parte precária de se defender mais facilmente nos procedimentos legais oriundos desta nova realidade[140].

Por último, aplicando o regime atual a este contexto algorítmico, a prática de um qualquer ato discriminatório lesivo não deixa de conferir o direito a uma indemnização por danos patrimoniais e não patrimoniais nos termos do art. 28º CT, devendo ser eficaz, proporcional e dissuasiva nos termos do arts. 15º e 17º da Diretiva 2000/43/CE, de 29 de junho e da Diretiva 2000/78/CE, de 27 de novembro respetivamente. De igual modo, recorda-se que no caso de candidato ilicitamente excluído, a obrigação de o admitir será uma solução jurídica inviável e de difícil execução no nosso ordenamento ao contundir com a natureza jurídica da prestação laboral, nomeadamente o cariz *intuito personae* e a liberdade de gestão empresarial, e ao limitar a autonomia privada e liberdade negocial do empregador, atentando contra a possibilidade de denúncia pelo mesmo durante o período experimental[141]. Diferentemente, no caso do trabalhador, o contrato já estaria em execução pelo que o empregador estaria obrigado à reconstituição natural da situação que existiria caso tal conduta não tivesse ocorrido.

---

140 Neste sentido, *vide* DATATILSYNET (Norwegian DPA), "Artificial intelligence and privacy", 2018, disponível em: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>, p. 23 e Martini, Mario, *Fundamentals of a regulatory system for algorithm-based processes - Expert opinion prepared on behalf of the Federation of German Consumer Organisations*, Speyer, 2019, pp. 35-37, este último A. apologista de que os controladores de dados teriam então de refutar a presunção de prova apresentando registos das sequências de processamentos do algoritmo, fornecendo provas de uma supervisão adequada dos processos técnicos ou desafiando de outra forma a presunção de causalidade.

141 A nível comparado, o ordenamento espanhol apresentou uma solução distinta no caso STSJ Islas Canarias, Las Palmas, secção 1, de 22.12.2008, resolução n.º 1860/2008, (Maria Garcia Hernandez) onde, para além da existência de indemnização durante um processo de seleção de pessoal, declarou a nulidade radical da conduta lesiva (*in casu*, a discriminação do candidato) e a reposição da situação no momento anterior a se produzir a violação do direito fundamental, impondo a obrigação de o contratar, ainda que a jurisprudência europeia nesta matéria (cfr. TJUE, *Von Colson e Kamann v. Land Nordrhein-Westfalen*, 10.04.1984, Case C-14/83) tenha vindo a defender que a contratação não deve ser exigida, sendo que o mais importante é que as indemnizações sejam eficazes, proporcionais e dissuasivas. Sobre este assunto, fazendo uma recensão de jurisprudência, *vide* Moll Noguera, Rafael, "La discriminación en el acceso al empleo público por razón de edad y su relación con las medidas positivas: cuestiones procesales y sustantivas a raíz de la STSJ C. Valenciana de 20.12.2018 (rec. 3174/2018)", *in*: *Labos*, Vol. 1, n.º 2, 2020, pp. 109-127.

6. Considerações finais

Tomando como emprestada a emblemática expressão de Ronald Reagan "*trust, but verify*", que utilizou o provérbio do inimigo Russo num contexto de Guerra Fria para descrever a abordagem das relações entre os EUA e a URSS, a verdade é que é possível utilizá-la como paralelo para a atual revolução digital iminente e sem igual[142] que traz questões sensíveis para as relações laborais, denotando-se uma verdadeira gestão digital do trabalho através do uso de algoritmos que acabam por estruturar silenciosamente a vida dos trabalhadores, pelo que apenas nos será possível confiar em sistemas automatizados decisores ao verificarmos e nos prevenirmos com o devido olhar atento que se exige. Tendo isto presente, de modo a eliminarmos as suas características de *WMDs* e fazer sobressair as suas qualidades, propõe-se atender ao a algumas ideias chave[143]:

I. Criar regulamentação e legislação sobre o uso dos algoritmos - como a Proposta de Regulamento Inteligência Artificial[144] ou a própria Resolução 2020/2012(INL)[145] - é imperativo, dado o alcance, universalidade e sensibilidade dos problemas registados, uma vez que o principal argumento contra a IA é motivado, legitimamente, pelo medo do desconhecido em contraste com a falta de adaptação legislativa neste campo, daí que a nossa lei atual (tal como na grande maioria dos países), não está ainda preparada para abordar casos desta

142 Nas palavras de Coelho Moreira, Teresa, op. cit., pp. 245-264, "esta revolução [digital] é diferente já que se atravessa um período de uma evolução sistémica excecional e raramente comparada a qualquer outra prévia. Não se trata de crise, mas de uma verdadeira metamorfose, não de passagem entre dois estados mais sim de um salto para o desconhecido".

143 Alguns dos pontos foram inclusive reforçados e enaltecidos nos arts. 9º e 14º da Carta Portuguesa de Direitos Humanos na Era Digital (Lei n.º 27/2021, de 17 maio), bem como pelo Livro Verde, "Sobre o futuro do Trabalho (trabalho, solidariedade e segurança social)", versão preliminar, junho 2021, disponível em: <https://www.portugal.gov.pt/pt/gc22/comunicacao/documento?i=livro-verde-sobre-o-futuro-do-trabalho>, pp. 47-54 e pp. 59-69 nos dados estatísticos apresentados e linhas de reflexão sobre a matéria.

144 Proposta de Regulamento do Parlamento Europeu e do Conselho COM(2021) 206 final, que estabelece regras harmonizadas em matérias de Inteligência Artificial, de 21.04.2021, disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206>.

145 Resolução (2020/2012(INL)) do Parlamento Europeu, que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas, de 20.10.2020, disponível em: <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_PT.html>.

natureza, pelo que se defende a procura de uma garantia de que a busca por maior produtividade não resulte na violação de direitos fundamentais, em riscos ocupacionais e repercussões a nível de saúde para os trabalhadores envolvidos como vimos no caso da *Amazon* ou da *Uber*. Assim, parece-nos fundamental padronizar aquilo que é admissível que seja programado, criando uma espécie de ética uniforme para os algoritmos e uma lei-modelo que cada E-M implementaria na sua legislação nacional, seguida de um relatório revelador de soluções e justificações adotadas no seu território enquanto possível técnica legislativa[146]. Nesta linha, as leis de combate à discriminação podem revelar-se nucleares ao fornecerem proteções importantes para os trabalhadores, sendo, por isso, necessária e urgente uma atualização e adaptação da legislação laboral[147] de modo a evitar que o lado mais frágil fique (ainda mais) vulnerável face à entrada rompante da IA no campo das relações laborais. A nível europeu esteve bem o RGPD em trazer algo à discussão que a Lei de Execução não foi capaz de vingar, tratando-se quanto a nós, de uma clara falha legislativa incapaz de estar a par dos tempos modernos da economia digital que a cada dia que passa vai intensificando os seus (velhos) problemas e criando novos sem apresentar respostas. De igual modo, os avanços tecnológicos são mais eficazes quando acompanhados por uma maior clareza quanto ao apuramento da responsabilidade algorítmica, qual o tipo que estará em causa e como se poderá reagir na prática perante este novo contexto, daí a importância da negociação e acordos coletivos por parte das organizações de trabalhadores e empregadores enquanto recurso basilar para o efeito, podendo (e devendo) contribuir para a solução de assuntos relacionados com o uso de tecnologia digital, coleta de dados e algoritmos que direcionam e disciplinam a força de trabalho procurando assegurar transparência e sustentabilidade social, sendo que a conformidade de tais práticas com a regulamentação pode, *rectius*, deve tornar-se um objetivo crucial de diálogo entre empregadores e trabalhadores[148]

146 Neste sentido, Kajtár, Edit e MESTRE, Bruno, *op. cit.*, pp. 241-243.

147 Neste sentido, Barzilay, Arianne Renan, & Ben-David, Anat, "Platform Inequality: Gender in the Gig-Economy", *in*: *Seton Hall Law Review*, Vol. 47, n.º 2, 2017, pp. 393-431, (pp. 429-430).

148 Enaltecendo o importante papel da negociação coletiva na flexibilização da regulamentação algorítmica e da sua adaptação à inovação tecnológica, *vide* De Stefano, Valerio, "Negotiating the Algorithm: Automation, Artificial intelligence and labour

permitindo afastar a dimensão puramente unilateral da governação do trabalho perante esta nova realidade.

II**.** A necessidade de uma *human in command approach.* Embora seja possível ter a IA a decidir questões como contratar trabalhadores, ou despedi-los, tais decisões devem ser sempre implementadas após uma abordagem de "ser humano no comando" defendida expressamente no seio comunitário[149] sendo, por isso, crucial que o ser humano permaneça legalmente responsável pela decisão e os consequentes efeitos nefastos[150], pelo que o fato das decisões

protection", *in*: *Comparative Labor Law & Policy Journal,* Vol. 41, n.º 1, 2019, pp. 1-32 ao salientar que os acordos coletivos poderiam tratar do uso de tecnologia digital, coleta de dados e algoritmos que direcionam e disciplinam a força de trabalho, garantindo transparência, sustentabilidade social e a conformidade dessas práticas com a regulamentação. Na mesma linha, *vide* atentamente o próprio Relatório OIT, *op. cit.*, pp. 42-44 juntamente com Todolí-Signes, Adrian, *op. cit.*, pp. 11-13 e Martini, Mario, *op. cit.*, pp. 39-41, sugerindo este último A., a criação de um Código de Responsabilidade Algorítmica que consistiria numa comissão governamental composta por representantes de trabalhadores e empregadores, empresas de software, administração pública, e cientistas com o intuito de formular recomendações sobre como os algoritmos devem ser utilizados em áreas sensíveis aos direitos fundamentais, como são exemplo as relações laborais.

149 Cfr. EESC, "Artificial Intelligence - The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society", Adopted on 31.05.2017, disponível em: <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/artificial-intelligence-consequences-artificial-intelligence-digital-single-market-production-consumption-employment-and>, p. 43. Aliás, o Parecer CESE, *op. cit.*, indica expressamente que a "pré-condição de que o desenvolvimento da IA seja responsável, seguro e útil, onde as máquinas permanecem máquinas e as pessoas mantêm o controle sobre essas máquinas a todo o tempo devem ser rigorosamente seguidos também em relação ao [âmbito] laboral" e, na mesma linha se pronuncia o Relatório OIT, *op. cit.*, p. 13, de que "potenciar e gerir a tecnologia a favor do trabalho digno, significa também adotar uma abordagem da IA baseada no "ser humano no comando", que garanta que decisões finais que afetem o trabalho sejam tomadas por seres humanos e não por algoritmos, [pois o] trabalho não é uma mercadoria".

150 Segundo o GT29º, *op. cit.*, p. 27, "[deve primar-se pela existência de] meios [que permitam] ao titular dos dados manifestar o seu ponto de vista e contestar a decisão (…) e um mecanismo de intervenção humana em casos definidos, [como] a disponibilização de uma hiperligação para um procedimento de recurso no momento da entrega da decisão automatizada ao titular dos dados, com os prazos de revisão acordados e o nome de um ponto de contacto para quaisquer dúvidas", e a verdade é que num estudo de investigação realizado por Fischer, Sarah & Petersen, Thomas, *Was Deutschland über Algorithmen weiß und denkt: Ergebnisse einer repräsentativen Bevölkerungsumfrage*, Bertelsmann Stiftung, 2018, pp. 24-30, cerca de 79% da opinião pública revelou que se encontra desconfortável e reticente quanto ao facto dos algoritmos julgarem as pessoas e tomarem decisões de forma instantânea e automatica, preferindo as decisões tomadas por pessoas por mais defeituosas e subjetivas que sejam. Nesta esteira, concedendo argumentos e razões do porquê de devermos confiar nas decisões humanas ao invés da *AI*, *vide* La Diega, Guido Noto, *op. cit.*, pp. 1-33 e Oddenino, Alberto, "Decisioni

serem tomadas após processos baseados em algoritmos nunca deve ser uma razão suficiente para excluir a responsabilidade humana nem que seja por uma questão de dignidade[151], conferindo ao demandante o direito de entrar em contato com um responsável humano de forma a poder reagir perante uma decisão que lhe foi desfavorável, de justificar e fundamentar devidamente a sua contestação, podendo exigir um direito de explicação que muitas vezes se revela paradoxal[152]. No fundo, devemos evitar uma abordagem de desumanização do trabalho por uma máquina omnipotente e omnipresente que o instrumentaliza e desvaloriza os valores humanos[153], uma nova realidade que deixa cicatrizes em termos de saúde física e mental[154] levando ao aumento de pressão, stress, ansiedade, depressão e até *burnout,* refletindo-se na qualidade da própria prestação do labor, podendo as tecnologias digitais fazer surgir novos riscos ou intensificar riscos profissionais já existentes.

III. Assegurar transparência e o direito à explicação é um ponto que não deve ser subestimado. A infra informação tecnológica[155] faz-se notar nos

algoritmiche e prospettive internazionali di valorizzazione dell'intervento umano", *in*: *DPCE online*, Vol. 42, n.º 1, 2020, pp. 199-217.

151 Como refere Zarsky, Tal Z., "Incompatible: The GDPR in the Age of Big Data", *in*: *Seton Hall Law Review*, Vol. 47, Issue 4, 2017, pp. 995-1020, (pp. 1016-1018), quando confrontado com decisões cruciais, um ser humano deve ser tratado com a dignidade de ter um decisor humano a tratar do seu assunto pessoal, não uma máquina.

152 Assiste-se a este paradoxo no caso da *Uber,* na qual os termos e condições globais do condutor de *Uber* preveem que os despedimentos automatizados têm lugar, mas ao mesmo tempo no seio europeu pregoa-se por um direito de contestar perante um ser humano. Sobre o assunto, *vide* Dencik, Lina, *et al.*, *op. cit.*, p. 467.

153 O mesmo será dizer que a dignidade é violada quando a pessoa deixa de ser considerada como um sujeito individual e um fim em si mesmo, sendo, ao invés, tratada como um instrumento ou um meio de realização de fins alheios.

154 Quanto aos possíveis riscos para a saúde dos trabalhadores como consequência da algocracy, vide a nível europeu o Relatório EU-OSHA, "Foresight on new and emerging occupational safety and health risks associated with digitalisation by 2025", 2018, disponível em: <https://osha.europa.eu/en/tools-andpublications/publications/foresight-new-and-emerging-occupational-safety-and-healthrisks/view>, pp. 55-57 e o Relatório OIT, "Seguridad y salud en el centro del futuro del trabajo", Ginebra, 2019, disponível em: <https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms_686762.pdf>, p. 31. Na doutrina, vide Todolí-Signes, Adrian, "Complying with the first law of robotics: An analysis of the occupational risks associated with work directed by an algorithm/artificial intelligence", in: SSRN, 2020, pp. 1-32, (pp. 14-19) e o interessante estudo de Popma, Jan, "The janus face of the "New ways of work", Rise, risks and regulation of nomadic work", in: SSRN, 2013, pp. 1-40, (p. 11), sobre o conceito de tecno-stress cindido em cinco elementos subjacentes: tecno-ansiedade, tecno-fadiga, tecno-adição, tecno-invasão e tecno-sobrecarga.

155 Aliás, num estudo levado a cabo por Fischer, Sarah & Petersen, Thomas, *op. cit.*,

dias correntes, i.e., a privação, desconhecimento e compreensão dos critérios e técnicas que estão a ser aplicados em determinada decisão algorítmica, impedindo o demandante de avaliar e reclamar fundadamente, fomentando a sua inércia perante resultados arbitrários e/ou discriminatórios sendo, por isso, imperativo que possa obter as respostas que procura. Deste modo, é importante reforçar que "explicabilidade" não é sinónimo de "transparência", na medida em que ser capaz de compreender o processo por meio do qual uma decisão foi tomada não é o mesmo que conhecer todos os passos tomados para atingir a mesma[156]. Nesta linha, o dualismo entre o direito à explicação *ex post* e o direito à informação geral *ex ante* deve ser superado, pelo que defendemos que aqueles dois conceitos devem fundir-se num único denominado de "legibilidade" devendo os trabalhadores ser capazes de compreender a importância e implicações do processamento algorítmico de dados e por que razão um sistema automatizado chegou a uma determinada decisão, o que também se revela importante em termos de apuramento de responsabilidade e transparência, existindo quem proponha um modelo de explicações contra factuais, ou seja, o dever de esclarecer os indivíduos visados por *ADMs* acerca do que teria de mudar para receber um resultado desejado no futuro com base no atual modelo de tomada de decisão[157]. Mais: a lei prevê um acesso a "informação significativa sobre a lógica envolvida", quererá isto significar que a lei exige uma explicação da funcionalidade do sistema (i.e., da lógica, significado, consequências previstas e funcionalidade geral) ou uma explicação de decisões específicas (i.e., da fundamentação, razões e circunstâncias)? Entendemos que a última abordagem será preferível pois em contexto, tal acesso parece associado ao direito de contestar uma decisão do n.º 3 do art. 22º RGPD[158] e, para o efeito, poderia recorrer-se ao campo da AI explicável ou *XAI*

---

pp. 12-15, quase metade dos inquiridos (45%) não conseguiu dar uma resposta clara acerca do conceito de algoritmo ou da própria IA em geral. Revela-se, por isso, bastante importante combater esta ignorância do homem médio relativamente aos algoritmos enquanto arma cada vez mais utilizada contra si mesmo.

156 Neste sentido, Ibnouhsein, Mohamed Issam, & Pégny, Maël, "Quelle transparence pour les algorithmes d'apprentissage machine?", 2018, pp. 1-34, disponível em: <https://hal.inria.fr/hal-01791021>, pp. 18-29.

157 A favor: Mittelstadt, Brent, *et al., op. cit.*, p. 4; Contra: Tabarrini, Camilla, *op. cit.*, pp. 135-143.

158 Neste sentido, POWLES, Julia & SELBST, Andrew D., *op. cit.*, p. 233.

cuja técnica apresenta um propósito de transparência, assumindo formas que possam ser compreendidas pelo ser humano[159].

Apesar dos algoritmos serem ferramentas úteis de auxílio ao empregador, não devem ser os fatores determinantes nas decisões que afetam os seus direitos vitais pelo que devemos ter em conta o explanado pela jurisprudência italiana ao elencar e munir o demandante de efetivas ferramentas de reação i.e., que um documento que inclui o algoritmo utilizado e a mera explicação da lógica em termos matemáticos e informações relativas à complexidade da construção e funcionamento do mesmo não atende, de *per si*, ao requisito legal, devendo antes ser interpretado como sendo necessária a divulgação do algoritmo com uma explicação em termos não técnicos da lógica da decisão e dos critérios em que se baseia, pois só desta forma o titular dos dados poderá contestar da melhor maneira a decisão e uma interpretação diferente não estaria em conformidade com o direito à ação e um processo equitativo, bem como o direito a um recurso efetivo nos termos dos par. 1º e 2º do art. 47º CDFUE e arts. 6º e 13º CEDH, que corresponde na nossa CRP, ao acesso ao direito e tutela jurisdicional efetiva do art. 20º CRP. Pregoamos assim por uma abertura segura da Caixa de Pandora, limitada, controlada, e acima de tudo, cognoscível na clareza do seu conteúdo pelo demandante. A não ser assim, sucede o que acontece em larga escala ao dia de hoje: o empregador, de forma consciente ou involuntária, subordina o seu controle e responsabilidade a um algoritmo com todos os riscos e perigos que isso representa, e os trabalhadores não podem exigir saber com que base, em que critério e com que peso e medida uma decisão algorítmica foi tomada contra si de modo a recorrer da mesma. No fundo, nunca devemos chegar à situação em que o empregador pode simplesmente encolher os ombros e dizer: "o algoritmo disse que o devia contratar ou despedir, mas não sei porquê". Portanto, para que um direito à

159 Cfr. Mittelstadt, Brent, RUSSEL, Chris & Wachter, Sandra, "Explaining explanations in AI", *in*: *FAT* '19: Proceedings of the Conference on Fairness, Accountability, and Transparency,* 2019, pp. 279-288, (pp. 279-288). Para mais desenvolvimentos, *vide* Vaquero De Miguel, Guillermo, *Aproximaciones a la Explicación de Decisiones Algorítmicas: Inteligencia Artificial Explicable*, Trabajo Fin de Grado, Universidad Politécnica de Madrid, 2020, pp. 47-53, trazendo à colação as técnicas da metodologia *XAI*, que dentro da área da IA são capazes de "abrir" a *black box* de certos algoritmos, facilitando, desta forma, a transparência e a compreensão do seu funcionamento interno.

informação sobre a lógica envolvida seja significativo deve ser mais do que uma simples regurgitação do *source code*, rejeitando-se a divulgação formal do código algorítmico balizado por *IP rights* e *trade secrets*[160] pois só uma adequada prestação da informação descodificando a efetiva *ratio* subjacente à decisão se demonstra coerente com o RGPD[161], conferindo materialmente informação útil que possibilite o demandante de reagir tornando o binómio transparência/privacidade numa dualidade.

IV. A premência da realização de auditorias ao algoritmo. A fiscalização algorítmica revela-se importantíssima para encontrar a justiça uma vez que permite "interrogar" os algoritmos de modo a alterá-los, aperfeiçoá-los e corrigi-los para serem melhores. Desta forma, propõe-se uma espécie de auditoria ao algoritmo[162] cujo processo poderá consistir essencialmente em:

Numa fase (pré) inicial, (i) o algoritmo deverá ter em conta particularidades e características do ser humano, de modo a evitar a sua coisificação, ou seja, a subjetividade acaba por interessar e ser relevante mas na medida certa,

---

160 Neste sentido, Powles, Julia & Selbst, Andrew D., *op. cit.*, pp. 233-242 e segundo a Datatilsynet (Norwegian DPA), *op. cit.*, pp. 21-22, "independentemente do significado das diferenças linguísticas, o responsável pelo tratamento deve fornecer tantas informações quantas as necessárias para que o sujeito dos dados possa exercer os seus direitos. Isto significa que a decisão deve ser explicada de modo a que a pessoa em causa possa compreender o resultado. O direito a uma explicação não significa necessariamente que a *black box* deve ser aberta, mas tem de permitir à pessoa em causa compreender por que razão foi tomada uma determinada decisão, ou o que precisa de ser alterado para que uma decisão diferente possa ser tomada". Entre nós, *vide* Cabral, "AI and the Right to Explanation: Three Legal Bases under the GDPR", *in*: *Data Protection and Privacy - Data Protection and Artificial Intelligence* (eds., Dara Hallinan, Ronald Leenes, Paul De Hert), Vol. 13, Hart Publishing, 2021, pp. 29-56.

161 Em França, a CNIL, "Comment Permettre à L´Homme de Garder La main? Les enjeux éthiques des algorithmes et de l´intelligence artificielle", 2017, disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf>, defendeu este princípio da transparência. Em Itália, LA DIEGA, Guido Noto, *op. cit.*, pp. 27-32 propõe como alternativa que se a decisão algorítmica for baseada em dados pessoais por uma entidade privada, este caminho é preferível, já se o tomador de decisão for uma entidade pública, deve optar-se por uma solicitação de FOIA com a justificação de que o sector público tutela interesses superiores e de maior gravidade, pelo que se permite essa ponderação acrescida.

162 Apologista desta ideia, desenvolvendo-a com grande pormenor e detalhe, vide Kim, Pauline T., "Auditing Algorithms for Discrimination", in: University of Pennsylvania Law Review, Vol. 166, Issue 1, 2017, pp. 189-203. De igual modo, trata-se de uma visão intensamente sugerida pela Administração Obama em 2016, quando se pronunciava sobre estes novos desafios relacionados com os sistemas algorítmicos (cfr. Obama Administration, "Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights", 2016, disponível em: <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf>, pp. 22-24).

devendo o algoritmo incorporar e ter em conta elementos que representem um risco para a segurança e a saúde dos trabalhadores e ser programado de forma a processar a informação que consiga reunir de modo a prevenir os possíveis riscos inerentes à respetiva prestação laboral da mesma maneira que um supervisor deve estar ciente dos perigos subjacentes ao posto de trabalho dos trabalhadores sob sua responsabilidade[163]. Para tal, parece necessário que a avaliação de risco obrigatória seja inserida na programação do algoritmo devendo, se possível, consultar-se os representantes dos trabalhadores de forma a estabelecer os critérios que o algoritmo deve seguir para gerenciar esse trabalho; (ii) deve procurar-se testar várias versões do *software* com casos reais previamente à sua utilização com a especifica finalidade de detetar preconceito e arbitrariedade[164] dado que nesse caso já haveria alternativas, devendo o responsável optar pela que fosse menos discriminatória e mais eficaz, permitindo clarificar a sua responsabilidade por falta desse cuidado pois a verdade é que o empregador ou mesmo a empresa que desenvolve o algoritmo muitas vezes não têm "incentivos" para proceder a estas avaliações minuciosas e morosas, ultrapassável por via da criação de um regime sancionatório por falta de cumprimento deste tipo de regras. Quem desenha o algoritmo precisa deste *feedback* de erro, de estudar os *outputs* maliciosos de modo a investigar e descobrir o que deu errado, o que foi mal lido, que dados foram ignorados, sendo desta maneira que os sistemas aprendem e se tornam mais inteligentes ao mesmo tempo que, paralelamente, precisam de *feedbacks* positivos de modo a terem conhecimento de que está efetivamente a resultar, de forma a melhorar

163 Neste sentido, Todolí-Signes, Adrian, *op. cit.*, pp. 23-24 e como refere La Diega, Guido Noto, *op. cit.*, p. 11, falta aos algoritmos a capacidade cognitiva e emocional de compreender uma situação da perspetiva do ser humano, uma vez que a empatia tempera os excessos legais.

164 Uma das estratégias da *HireVue* como forma de mitigar preconceitos consiste na eliminação de indicadores que têm um impacto adverso nos grupos protegidos, em que as características que provocam resultados tendenciosos são removidas e os modelos são re-treinados e reavaliados até que o viés não seja detetado (cfr. <https://www.hirevue.com/why-hirevue/ethical-ai>). Nesta linha encontra-se o GT29º, op. cit., p. 32 ao defender a "existência de controlos periódicos de garantia da qualidade dos respetivos sistemas a fim de assegurar um tratamento equitativo e não discriminatório das pessoas (…) e obter garantias contratuais (…) de que o controlo e os testes foram efetuados e que o algoritmo está conforme às normas aceites. Estas medidas deverão ser utilizadas de modo cíclico, ou seja, não apenas na fase de conceção, mas também permanentemente enquanto for aplicada uma definição de perfis às pessoas".

e aprimorar o algoritmo[165]; (iii) considerar o rigor e a *accuracy,* i.e., aferir com que frequência o algoritmo falha, com quem falha e qual é o custo dessa falha, devendo os empregadores de ser capazes de compreender *e.g.,* a razão de um candidato ter sido rejeitado, e nesta linha, tomar em consideração os ciclos viciosos das decisões algorítmicas, os efeitos perniciosos a longo prazo, parálos e modificá-los, aferindo se o algoritmo usado e desenvolvido pelo sistema de *ML* está a produzir resultados discriminatórios, arbitrários e injustificados.

Numa fase final, (iv) fiscalizar a integridade dos dados através de uma espécie de posição original de Rawls[166] a partir do qual se levanta o "véu de ignorância" ao nos colocarmos numa "prova às cegas"[167] afastando qualquer preconceito *ab initio* na fase de recrutamento, daí a importância de reformular a coleta histórica de informação que serve de *input* uma vez que um algoritmo é tão bom quanto os dados com os quais trabalha; **(v)** garantir imparcialidade nessa auditoria - acolhendo a proposta da doutrina alemã e italiana[168] - por via da criação de um órgão independente que seja capaz de o fazer regularmente, se possível através da contratação de especialistas independentes, grupos de direitos humanos para o efeito ou atribuindo-se a empresas de fora o poder de recrutamento com a devida fiscalização por parte da Autoridade para as Condições do Trabalho (ACT). Por outro lado, poderá ainda desenvolver-se a criação de um sistema de deteção de discriminação incorporado na própria

165 Cfr. O´Neil, Cathy, *op. cit.*, pp. 133 e 209; Kleinberg, Jon, *et al.*, *op. cit.*, pp. 144-145 e Edwards, Lilian & Veale, Michael, "Enslaving the algorithm: from a right to an explanation to a right to better decisions"?, *in*: *IEEE Security & Privacy*, Vol. 16, n.º 3, 2018, pp. 46-54.

166 Rawls, John, *A Theory of Justice*, Oxford University Press, 1972, pp. 17-22.

167 Neste sentido, *vide* Goldin, Claudia & Rouse, Cecilia, "Orchestrating Impartiality: The Impact of Blind Auditions on Female Musicians", *in*: *American Economic Review*, Vol. 90, n.º 4, 2000, pp. 715-741, (pp. 737-738) e O´Neil, Cathy, *op. cit.*, pp. 113-115, recorrendo ao exemplo das *blind orquestra auditions* que na década de 1970 estiveram em destaque ao iniciarem um movimento caracterizado pela realização de audições com o músico escondido atrás de uma partitura, levando a que reputações e interesses subjetivos que provocavam injustiças passassem a não ter qualquer valor na critério de recrutamento e avaliação, a par da etnia, do género ou mesmo da *Alma Mater* do músico, demonstrando que, desde então, a percentagem de mulheres que tocam em grandes orquestras deu um salto quantitativo aumentando em cerca de 5x recorrendo a este método, sendo deste modo que é invocada e utilizada como bom presságio para o paralelo *sub judice.*

168 Cfr. respetivamente, Barocas, Solon & Selbst, Andrew D., *op. cit.*, pp. 682-701 e FLORIDI, Luciano, *et al., op. cit.*

ML de modo a preveni-la[169]. Deste modo, relativamente à controvérsia questão que envolve os *trade secrets* e *IP rights*, reforçamos o entendimento de que, mesmo que uma empresa reclame que o algoritmo é propriedade sua e que, por isso, deve ser mantido em segredo, ainda assim deve-lhe ser exigido que ofereça testes robustos para que especialistas externos possam examinar o seu desempenho[170].

Tendo presente estas considerações, revela-se importante o contributo que o RGPD vem trazer com a criação da avaliação do impacto sobre a proteção de dados (AIPD), atuando como mecanismo *ex ante* ao permitir que os controladores avaliem e determinem se existe o risco de uma qualquer discriminação, parcialidade ou erro e, caso isso aconteça, desenvolver medidas para minimizar os danos potenciais, sendo também utilizada para informar a pessoa em causa sobre a lógica subjacente a um processo de *ADM* permitindo-lhe opor-se à decisão e/ou expressar o seu ponto de vista, enquanto processo contínuo e não isolado no tempo. De igual modo, a sua utilização obrigará as organizações a demonstrar a necessidade e proporcionalidade de um qualquer tratamento de dados pessoais relacionados com a IA, a prestar contas de algum prejuízo que possa resultar de uma certa parcialidade ou inexatidão de um sistema e a explicar a lógica subjacente a um necessário *trade-off* entre transparência/privacidade. As AIPDs podem também auxiliar organizações a ponderar sobre as melhores formas de prevenir os riscos mais amplos de danos a trabalhadores ou as implicações éticas para a sociedade em geral[171], tentando

169 Neste sentido, propondo a criação de uma ferramenta algorítmica anti discriminatória incorporada no próprio sistema de *ML*, *vide* Feldman, Michael, Friedler, Sorelle A., Moeller, John, Scheidegger, Carlos, & Venkatasubramanian, Suresh, "Certifying and Removing Disparate Impact", *in*: *KDD '15: Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2015, pp. 259-268; Bornstein, Stephanie, *op. cit.*, p. 1110 e Masseno, Manuel David e Santos, Cristiana, "Assuring Compliance of European Smart Tourist destinations with the principles of the general data protection regulation: a roadmap", *in*: *Anuário de Proteção de Dados,* (coord. Francisco Pereira Coutinho, Graça Canto Moniz), CEDIS, 2019, pp. 87-108, (pp. 95-107).

170 Veja-se o exemplo da *Pymetrics* que desenvolveu a ferramenta específica *audit-A* para realizar auditorias ao algoritmo e lançou-a como um *software* de código aberto (cfr. <https://github.com/pymetrics/audit-ai>).

171 Neste sentido encontra-se o GT29º, *op. cit.*, pp. 26-30, onde embora reforce que o "objetivo de tal processo seria ajudar a fomentar a confiança nas operações de processamento do controlador, e demonstrar responsabilidade e transparência", entende que a publicação de AIPD´s não é um requisito legal do RGPD. Criticando esta posição, *vide* Tuncay, Bilgesu,

corrigir as falhas do algoritmo, respeitando o disposto no art. 25º RGPD e promovendo a proteção de dados desde a conceção e por defeito. Nesta linha, a alínea a) do n.º 3 do art. 35º RGPD destaca a necessidade e obrigatoriedade de o responsável pelo tratamento proceder a uma AIPD (cfr. Considerando (90)) em caso de *ADMs* e definição de perfis, exigindo que o responsável afira dos riscos envolvidos neste campo, podendo igualmente constituir um meio útil de identificação das medidas a introduzir para combater os perigos em matéria de proteção de dados resultantes do tratamento[172], entre as quais: **(a)** informar o titular dos dados da existência de um processo de *ADM* e da lógica subjacente; **(b)** explicar-lhe a importância e as consequências previstas do tratamento; **(c)** proporcionar-lhe meios de se opor à decisão; **(d)** e permitir que manifeste o seu ponto de vista. Porém, não obstante a introdução deste mecanismo, defendemos uma fiscalização a dois tempos de forma complementar[173], quer *ex ante* (informações genéricas, enquanto atuação preventiva em que se procura evitar ou minorar a ocorrência de danos), quer *ex post* (informações especificas, quando o dano já ocorreu), na medida em que uma intervenção prévia a ser tomada a decisão[174] se revela uma ferramenta importante a par da análise realizada *a posteriori*[175].

Scrutinizing Algorithms for Unlawful and Undesirable Discrimination in Automated Decision-Making: An Analysis of Algorithm Audits and the GDPR, Tilburg Institute for Law, Technology, and Society, 2019, pp. 37-38, afirmando que mesmo que as organizações ou empresas não revelem as suas AIPD´s, o resultado das auditorias algorítmicas deve ser tornado público.

172 Nesta linha, em cumprimento do n.º 4 do art. 35º e ao abrigo da alínea k) do n.º 1 do art. 57º ambos do RGPD, a CNPD, por via do RE n.º 1/2018, DR 2ª Série, n.º 231, de 30.11.2018, veio estabelecer a lista de tratamentos de dados pessoais sujeitos a AIPD, devendo a avaliação incluir a descrição sistemática das operações de tratamento previstas e a sua finalidade, a avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos, a avaliação dos riscos para os direitos e liberdades dos titulares dos direitos e as medidas previstas para fazer face aos riscos.

173 Neste sentido, Bourke, Georgina, Carfantan, Paul-Marie, Eichholzer, Annalisa, Hutchinson, Ian, Joshi, Arnav & Powell, Alison, "Understanding and Explaining Automated Decisions", *in*: *SSRN*, 2019, pp. 1-28, (pp. 6-12 e 13-18); Besse, Philippe, *op. cit.*, p. 6 e Medon, Filipe, & Teffé, Chiara Spadaccini de, *op. cit.*, p. 303.

174 Solução defendida e desenvolvida por Bogen, Miranda & Rieke, Aaron, *op. cit.*, p. 45 ao ser implementada no (seu) ordenamento esloveno.

175 Apologistas desta solução isolada, *vide* Comandé, Giovanni, & Malgieri, Gianclaudio, *op. cit.*, pp. 243-265; Flaxman, Seth & Goodman, Bryce, "European Union regulations on algorithmic decision-making and a right to explanation", *in*: *AI Magazine,* Vol. 38, n.º 3, 2017, pp. 50-57 e KIM, Tae Wan & ROUTLEDGE, Bryan, *Algorithmic Transparency, a Right to Explanation, and Trust*, Carnegie Mellon University, 2017, pp. 1-31.

Administração eletrónica, eficiência e proteção de dados: breves considerações à luz dos princípios gerais da atividade administrativa

JOEL A. ALVES[*]

Resumo: Numa época em que a transição digital se processa a um ritmo cada vez mais acelerado, o presente artigo procura refletir sobre a seguinte questão de fundo: como compatibilizar (i) a incorporação de novas tecnologias na Administração Pública, a fim de garantir uma mais eficiente satisfação das necessidades coletivas, com (ii) a proteção conferida a cada cidadão relativamente ao tratamento de dados pessoais que lhe digam respeito?

Palavras-chave: *Administração Pública; eficiência; proteção de dados pessoais; transição digital; administração eletrónica.*

Abstract: At a time when digital transformation is proceeding at an even-increasing pace, the present article aims to reflect about the following question of substance: how to conciliate (i) the incorporation of new technologies in the Public Administration, in order to ensure a more efficient satisfaction of the collective needs, with (ii) the protection accorded to each citizen in relation to the processing of personal data concerning him or her?

Keywords: *Public Administration; efficiency; personal data protection; digital transition; electronic administration.*

---

[*] Assistente Convidado na Escola de Direito da Universidade do Minho. Investigador-bolseiro do JusGov – Centro de Investigação em Justiça e Governação da Universidade do Minho, no âmbito do projeto «Smart Cities and Law, E.Governance and Rights: Contributing to the definition and implementation of a Global Strategy for Smart Cities», IP Isabel Celeste M. Fonseca, ref. NORTE-01-0145-FEDER-000063. Doutorando em Ciências Jurídicas, na especialidade de Ciências Jurídicas Públicas, na Escola de Direito da Universidade do Minho.

1. Enquadramento

Falar de Administração Pública hoje, é falar de administração eletrónica[1]. Se dúvidas houvera a este respeito, a situação de emergência (sanitária, económica e social) provocada pelo vírus SARS-COV-2 e pela doença COVID-19 veio certamente dissipá-las.

Com efeito, a realidade é clara: seja ao nível da gestão documental e da tramitação dos procedimentos[2]; seja no âmbito do relacionamento com os particulares[3] e do funcionamento interno dos órgãos colegiais[4]; seja ainda, na prática de atos jurídicos[5], ou simples operações materiais[6], raros são os casos em que a tecnologia não se demonstra presente na atividade administrativa dos nossos tempos. Cenário que, fruto das prioridades políticas recém-estabelecidas, a nível nacional e europeu, em matéria de transição digital, parece, aliás,

1 Nesse sentido, cfr. Delgado, Isaac Martín, "El acceso electrónico a los servicios públicos: hacia um modelo de administración digital autenticamente inovador", in *Sociedad Digital y Derecho,* Imprensa Nacional del Boletín Oficial del Estado, 2018, p. 180.

2 Caso paradigmático é o que se verifica, entre nós, ao nível da contratação pública; domínio setorial onde, desde 2008, a desmaterialização é a regra. Para mais desenvolvimentos, cfr. Gonçalves, Pedro, *Direito dos Contratos Públicos*, 4.ª edição, Almedina, 2021, pp. 653 e ss.

3 Veja-se o que sucede no quadro das comunicações entre Administração e particulares, as quais são crescentemente realizadas com recurso a ferramentas digitais como o correio eletrónico; formulários online; plataformas de mensagens instantâneas; etc. Ferramentas essas que, a breve trecho, tenderão a ser acompanhadas por mecanismos ainda mais inovadores, como sejam robôs de conversação, suscetíveis de simular verdadeiros diálogos entre Homem e máquina. Nesse sentido, cfr. Flamínio da Silva, Artur, "Inteligência Artificial e Direito Administrativo", in *Direito Administrativo e Tecnologia*, Almedina, 2021, p. 16.

4 Reflexo disso, é a circunstância de muitas das reuniões desses órgãos se realizarem, hoje, através de meios telemáticos, tais como sistemas de tele e videoconferência. O que, recorde-se, o novo art. 24.º-A do Código do Procedimento Administrativo expressamente autoriza "sempre que as condições técnicas o permitam".

5 É, a este respeito, particularmente significativa a experiência da Alemanha; país onde a emissão de atos administrativos, gerados através de processos totalmente digitais e automatizados, é já admitida, nos casos em que exista uma norma habilitante para o efeito e a Administração não disponha de qualquer margem de discricionariedade ou livre apreciação. Para mais desenvolvimentos, cfr. Buoso, Elena, "Fully automated administrative acts in the German legal system", European Review of Digital Administration & Law, vol. 1, n.ºs 1-2, 2020, pp. 114 e ss.

6 Pense-se, desde logo, na lecionação de aulas; tarefa que, sobretudo na sequência dos constrangimentos provocados pelo vírus SARS-CoV-2 tem vindo a realizar-se (não só, mas também) através de canais digitais.

destinado a adquirir contornos de cada vez maior expressividade[7].

Ora, se tudo isto encerra inegáveis vantagens, permitindo aos órgãos e agentes administrativos prosseguirem o interesse público com um grau de eficiência e eficácia sem qualquer tipo de precedentes, a verdade, porém, é que nem tudo são rosas[8]. Afinal, cumpre ter presente que a *tecnologificação* da Administração Pública abre igualmente a porta a que esta disponha de capacidades de recolha, processamento, armazenamento e interconexão de informações nunca antes conhecidas[9]. O que, naturalmente, faz também aumentar (de forma substancial) o risco de violação dos direitos e liberdades fundamentais dos cidadãos[10] – ou não fossem a generalidade das informações tratadas pela Administração dados pessoais[11], e amiúde, dados pessoais de carácter altamente sensível[12].

Neste contexto, questão que forçosamente se coloca é a seguinte: como aproveitar o progresso da ciência e da técnica, de modo a melhor satisfazer as necessidades da coletividade, sem com isso diminuir a proteção conferida a cada um dos seus membros, contra o tratamento indevido de informações de carácter pessoal que lhes digam respeito? Dito de outro modo, numa versão renovada de um dos mais intrincados desafios a que o Direito Administrativo, desde sempre, procura dar resposta[13]: como compatibilizar as exigências da

---

7 Sobre o tema, cfr., com especial interesse, Fonseca, Isabel Celeste M., "Governação Pública Digital e a Proteção de Dados Pessoais: notas breves sobre as dificuldades de harmonização", in *Estudos de E.Governação, Transparência e Proteção de Dados*, Almedina, 2020, pp. 9 e ss.

8 Alertando para tal circunstância, cfr. Alves, Joel A. / Fonseca, Isabel Celeste M., "Legal developments on Smart Public Governance and Fundamental Rights in the Digital Age", in *Legal Developments on Cybersecurity and Related Fields*, Springer (no prelo).

9 Para mais afloramentos, cfr. Carullo, Gherardo, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, 2017, pp. 7 e ss. e 21 e ss.

10 Nesse sentido, cfr. Reigada, Antonio Trancoso, "La Administración Electrónica y la Protección de Datos Personales", *Revista Jurídica de Castilla y León*, n.º 16, 2008, pp. 59-60; Mañas, José Luís Piñar, "Administración Eléctronica y Protección de Datos Personales", *Dereito. Monográfico: Estudios sobre la modernización administrativa*, 2011, pp. 148 e 164.

11 Cfr. Auby, Jean-Bernard, "Administrative Law facing digital challenges", *European Review of Digital Administration & Law*, vol. 1, n.ºs 1-2, p. 9.

12 Idem, ibidem.

13 Sustentando que "aquilo que caracteriza genericamente o Direito Administrativo é a procura permanente de harmonização das exigências da ação administrativa, na prossecução de interesses gerais, com as exigências de garantia dos particulares, na defesa dos seus direitos e interesses legítimos»", cfr. Freitas do Amaral, Diogo, *Curso de Direito Administrativo*,

ação administrativa eletrónica, na prossecução de interesses gerais, com os imperativos de garantias dos particulares, na defesa do seu direito à proteção de dados pessoais?

No presente artigo, procurar-se-á, assim, apresentar o enquadramento principiológico pelo qual se deve nortear a Administração Pública na resposta a tão complexa problemática, avançando linhas orientadoras, suscetíveis de permitir a concretização daquele que subsiste como o seu primordial objetivo: realizar o interesse coletivo e impedir o esmagamento dos interesses individuais[14]. Enfim: prosseguir o interesse público, mas sempre no respeito pelos direitos e interesses legalmente protegidos dos cidadãos[15].

2. Administração Pública (Eletrónica) e Eficiência

2.1 O princípio da prossecução do interesse público

Independentemente daquilo que se entenda por Administração Pública, ponto é que esta se demonstra teleologicamente orientada, de forma *permanente* e *exclusiva*, pela realização do *interesse público*[16] – assim o determinam a 1.ª parte do n.º 1 do art. 266.º da Constituição da República Portuguesa ("a Administração Pública visa a prossecução do interesse público"), bem como a 1.ª parte do art. 4.º do Código do Procedimento Administrativo ("compete aos órgãos da Administração Pública prosseguir o interesse público").

Significa isto, que a Administração existe, atua e funciona com um único objetivo: garantir e promover o bem comum da coletividade[17], ou mais precisamente, assegurar a satisfação de todas aquelas necessidades que o legislador define como indispensáveis para a realização desse bem comum[18],

---

vol. 1, 4.ª edição, Almedina, 2016, p. 141.

14 Idem, p. 138.

15 Cfr. o n.º1 do art. 266.º da Constituição da República Portuguesa, bem como o art. 4.º do Código do Procedimento Administrativo.

16 Nesse sentido, cfr., por todos, Gonçalves, Pedro, *Manual de Direito Administrativo*, Almedina, 2019, p. 398.

17 Cfr. Otero, Paulo, *Direito do Procedimento Administrativo,* vol. 1, 1.ª edição, Almedina, 2019, pp. 153-154.

18 E é assim, pois que, como ensina Vieira de Andrade, "o interesse público não se impõe à Administração como fórmula abstrata de bem comum"; antes se lhe coloca "através das suas concretizações jurídicas normativas de nível constitucional ou legislativo". Daí que, em

tendo por referência as prioridades estabelecidas pela comunidade política em cada momento histórico[19]. É este "o seu norte, o seu guia, o seu fim"[20].

Daqui decorre que toda a atividade administrativa surge condicionada por dois limites fundamentais: (i) um *limite negativo*, expresso na proibição dos órgãos e entes administrativos motivarem as respetivas condutas por *interesses de carácter privado*[21], ou tão-só, por *interesses de natureza pública* que não se encontrem expressamente colocados por lei a seu cargo[22];

---

rigor, os órgãos e entes administrativos, no exercício da função administrativa, não prossigam o bem comum enquanto realidade geral e indiferenciada – aquilo que a Doutrina qualifica como o "interesse público primário" –, mas sim um conjunto restrito e pré-determinado de finalidades, às quais se reconhece instrumentalidade direta para a realização desse bem comum – os vulgarmente designados "interesses públicos secundários" (cfr. Vieira de Andrade, José Carlos, "Interesse Público", in *Dicionário Jurídico da Administração Pública*, Volume V, 1993, p. 280). Para mais desenvolvimentos, cfr., para além do autor já citado, Soares, Rogério, *Interesse público, legalidade e mérito*, 1953, pp. 99 e ss.; Fonseca, Isabel Celeste M., *Curso de Direito Administrativo. Teoria Geral da Organização Administrativa*, GestLegal, 2020, pp. 21 e ss.; Dias, José Eduardo Figueiredo / Oliveira, Fernanda Paula, *Noções Fundamentais de Direito Administrativo,* 5.ª edição (reimpressão), Almedina, 2021, pp. 17-19.

19 Alertando para a circunstância de o interesse público não constituir uma realidade estática, mas antes uma construção influenciada pelas contingências (políticas, económicas; sociais, culturais etc.) do seu tempo, cfr. Freitas do Amaral, Diogo, *Curso de Direito Administrativo*, vol. II, 4.ª edição, Almedina, 2020, p. 34; Otero, Paulo, *Manual de Direito Administrativo,* vol. I, 2.ª reimpressão da edição de 2013, Almedina, 2016, p. 69; Rebelo de Sousa, Marcelo / Salgado Matos, André, *Direito Administrativo Geral*, Tomo I, 3.ª edição (reimpressão), Publicações Dom Quixote, 2010, p. 41; Maurer, Hartmut, *Derecho administrativo alemán* (tradução espanhola), 1.ª edição, Universidad Nacional Autónoma de México, 2012, pp. 5-6; Casado, Eduardo Gamero / Ramos, Severiano Fernández, *Manual Básico de Derecho Administrativo*, 18.ª edição, Tecnos, 2021, p. 88.

20 Cfr. Freitas do Amaral, Diogo, *Curso de Direito Administrativo*, vol. II, 4.ª edição, Almedina, 2020.

21 É certo que a atividade administrativa poderá traduzir-se em escolhas coincidentes com os interesses privados dos seus destinatários (pense-se, designadamente, nos casos em que os órgãos da Administração Pública emitem uma licença de construção, requerida por um determinado particular). Não obstante, importante é que seja o interesse público e não um interesse privado a constituir a finalidade visada pela Administração com a realização das suas escolhas (no exemplo apresentado, a meta da atividade administrativa será velar pela conformidade do projeto de construção em causa com o quadro jurídico aplicável; não conceder uma vantagem ou benefício a um dado particular). Para mais desenvolvimentos, socorrendo-se do caso prático pré-enunciado, cfr. Rebelo de Sousa, Marcelo / Salgado Matos, André, *Direito Administrativo Geral*, Tomo I, 3.ª edição (reimpressão), Publicações Dom Quixote, 2010, pp. 46 e 208.

22 Cfr. Freitas do Amaral, Diogo, *Curso de Direito Administrativo*, vol. II, 4.ª edição, Almedina, 2020, p. 35; Rebelo de Sousa, Marcelo / Salgado Matos, André, *Direito Administrativo Geral*, Tomo I, 3.ª edição (reimpressão), Publicações Dom Quixote, 2010, pp. 46-47 e 208.

e (ii) um *limite positivo*, traduzido na atribuição a estas estruturas de um verdadeiro "direito-poder-dever"[23], no que diz respeito à satisfação de certos interesses, considerados essenciais para a coletividade[24]. Dito de outro modo: a Administração apenas pode prosseguir *interesses* que a lei qualifique como *públicos*[25]*;* porém, definindo a lei um interesse como público, a Administração tem forçosamente de prossegui-lo[26].

2.2 O princípio da boa administração

Sucede que, num Estado Social de Direito – tal como o é, jurídico-constitucionalmente, a República Portuguesa[27] – a Administração Pública não pode pura e simplesmente limitar-se a prosseguir este desígnio de qualquer maneira[28]. Pelo contrário: a concretização de uma verdadeira democracia económica, social e cultural pressupõe, numa realidade de recursos escassos, a vinculação das entidades administrativas às soluções que melhor assegurem a satisfação das suas missões em cada caso concreto[29]. Numa palavra: à Administração, não se lhe exige apenas que prossiga o interesse público;

---

23 Cfr. Colaço Antunes, Luís Filipe, *O Direito Administrativo e a sua justiça no início do século XXI*, Almedina, 2001, p. 42.

24 *Idem*, *ibidem*.

25 Com efeito, nem poderia ser de outra forma. É que, se por um lado, a Administração *visa a prossecução do interesse público*, nos termos previamente explicados; por outro lado, esta encontra-se *subordinada à Constituição e à lei*, ao abrigo do disposto no artigo 266.º/2 da Constituição da República Portuguesa. Donde, a afirmação *supra* se apresente como um simples corolário lógico, resultante da interligação sistemática do *princípio da prossecução do interesse público* com o (igualmente importante) *princípio da juridicidade*.

26 Cfr. Freitas do Amaral, Diogo, *Curso de Direito Administrativo*, vol. II, 4.ª edição, Almedina, 2020, p. 35; Soares, Rogério, *Interesse público, legalidade e mérito*, tese de doutoramento, 1953, p. 118; Caupers, João, *Introdução ao Direito Administrativo*, 5.ª edição, Âncora editora, 2000, p. 63.

27 Cfr. art. 2.º da Constituição da República Portuguesa, lido em articulação com o art. 9.º/*d)* do mesmo diploma. Para mais afloramentos, cfr. Canotilho, José Joaquim Gomes / Moreira, Vital, *Constituição da República Portuguesa Anotada,* vol. II, 4.ª edição, Coimbra editora, 2010, pp. 209-211 e 278.

28 Cfr. Viana, Cláudia, "O princípio da eficiência: a eficiente eficácia da Administração Pública", in *Revista da Faculdade de Direito da Universidade do Porto*, vol. 7, 2010, pp. 302 e ss.

29 Idem, p. 303. Em sentido próximo, cfr. Otero, Paulo, *Manual de Direito Administrativo,* vol. I, 2.ª reimpressão da edição de 2013, Almedina, 2016, p. 354; Freitas do Amaral, Diogo, *Curso de Direito Administrativo*, vol. II, 4.ª edição, Almedina, 2020, p. 34.

antes se lhe impõe que realize o *melhor interesse público possível*[30], o *ótimo interesse público*[31].

É pois, neste quadro, que o art. 5.º do Código do Procedimento Administrativo consagra o chamado *princípio da boa administração*, o qual estabelece: (i) a montante, que a Administração Pública deve pautar a sua atividade por critérios de eficiência, economicidade e celeridade[32]; (ii) e a jusante, que esta deve ser internamente organizada de modo a aproximar os serviços das populações e evitar expedientes burocráticos desnecessários[33].

Subjacente a este comando normativo apresentam-se, assim, duas dimensões bastante diversas[34], conquanto identicamente relevantes: (i) uma *dimensão funcional*, ancorada na premissa de que a ação administrativa deve ser desenvolvida com recurso aos meios técnica e financeiramente mais adequados para o atingimento dos respetivos fins[35], demorando menos

30 Cfr. Viana, Cláudia, "O princípio da eficiência: a eficiente eficácia da Administração Pública", in *Revista da Faculdade de Direito da Universidade do Porto*, vol. 7, 2010, p. 304.

31 Cfr. Otero, Paulo, *Direito do Procedimento Administrativo,* vol. 1, 1.ª edição, Almedina, 2019, pp. 155 e 271-272.

32 Cfr. o n.º 1, do art. 5.º, do Código do Procedimento Administrativo.

33 Cfr. o n.º 2, do art. 5.º, do Código do Procedimento Administrativo. Refira-se que, em rigor, o preceito em causa estabelece que "a Administração Pública deve ser organizada de modo a aproximar os serviços das populações e *de forma não burocratizada*" (sublinhado nosso). Não obstante, razão parece-nos ter Cabral de Moncada quando refere que "o que o código pretende evitar não é a burocracia, mas sim os seus excessos capazes conduzir a disfunções" (cfr. Cabral de Moncada, Luís, Código do Procedimento Administrativo anotado, Coimbra editora, 2015, p. 82). Daí que sigamos de perto a posição sustentada pelo autor.

34 Nesse sentido, cfr. Aroso de Almeida, Mário, *Teoria Geral do Direito Administrativo*, 6.ª edição, Almedina, 2020, pp. 129-130.

35 Identificando a adequação entre meios e fins como uma das características mais vincadas do conceito de eficiência (conceito esse, entendido em sentido amplo, enquanto expressão da tríade eficiência, economicidade e celeridade), cfr. Raimundo, Miguel Assis, "Os princípios no CPA e o princípio da boa administração, em particular", in *Comentários ao Código do Procedimento Administrativo*, vol. I, 5.ª edição, AAFDL editora, 2020, p. 329. Em sentido idêntico, cfr. Aroso de Almeida, Mário, *Teoria Geral do Direito Administrativo*, 6.ª edição, Almedina, 2020, p. 135; Gonçalves, Pedro, *Manual de Direito Administrativo*, Almedina, 2019, p. 398; Dias, José Eduardo Figueiredo / Oliveira, Fernanda Paula, *Noções Fundamentais de Direito Administrativo,* 5.ª edição (reimpressão), Almedina, 2021, p. 36; Tavares da Silva, Suzana, "O princípio (fundamental) da eficiência", in *Revista da Faculdade de Direito da Universidade do Porto*, vol. 7, P. 519; Viana, Cláudia, "O princípio da eficiência: a eficiente eficácia da Administração Pública", in *Revista da Faculdade de Direito da Universidade do Porto*, vol. 7, 2010, p. 301; Casado, Eduardo Gamero / Ramos, Severiano Fernández, *Manual Básico de Derecho Administrativo*, 18.ª edição, Tecnos, 2021, p. 95; Casetta, Elio, *Manuale di Diritto Amministrativo*, 22.ª edição, Giufrè Francis Lefebvre, 2020,

tempo[36], implicando menos custos[37], e, em última análise, pugnando por uma relação tendencialmente perfeita entre objetivos fixados, recursos (materiais e humanos) mobilizados e resultados conseguidos[38]; e (ii) uma *dimensão organizatória*, condensada no ideal programático[39], segundo o qual a Administração deve ser instrumentalmente estruturada com vista a assegurar a efetivação daqueles primeiros propósitos[40].

---

p. 54.

36 Ainda que não se esgotando nesse domínio, tal imposição reveste-se de particular importância no campo da atividade administrativa procedimental. Veja-se, a título de exemplo, o disposto no art. 59.º do Código do Procedimento Administrativo, preceito nos termos do qual se estabelece que "o responsável pela direção do procedimento e os outros órgãos intervenientes na respetiva tramitação devem providenciar por um andamento rápido e eficaz, quer recusando e evitando tudo o que for impertinente e dilatório, quer ordenando e promovendo tudo o que seja necessário a um seguimento diligente e à tomada de uma decisão dentro de prazo razoável". Nesse sentido, defendendo que "o domínio preferencial da aplicação do princípio da boa administração diz (...) respeito a situações de responsabilidade da Administração por morosidade excessiva na condução dos procedimentos e na tomada de decisões", cfr. Aroso de Almeida, Mário, *Teoria Geral do Direito Administrativo*, 6.ª edição, Almedina, 2020, p. 131.

37 Importa, todavia, salientar que esta exigência não pode ser perspetivada à luz de uma lógica absolutista, que conceba a minimização da despesa enquanto um objetivo dotado de prioridade automática sobre quaisquer outros interesses ou valores jurídico-comunitários. É que, casos poderá haver em que o meio mais económico, de entre aqueles que se encontram disponíveis, não coincida com a alternativa mais célere ou mais eficiente (em sentido estrito). Donde, a imposição de que a atividade administrativa se desenvolva através dos meios que impliquem menores custos, não se confunda com um simples mandato de procura pelo mais barato. Afinal, para o princípio da boa administração, a solução mais económica não tem necessariamente de revelar-se a solução menos dispendiosa, mas antes aquela que configura a melhor opção administrativa, do ponto de vista da relação custos/benefícios. Sustentando uma posição idêntica, cfr. Costa, Jorge / Pinto, Eliana de Almeida / Silva, Isabel Código do Procedimento Administrativo Comentado, Quid Iuris, 2018, p. 52.

38 Em sentido próximo, cfr. Otero, Paulo, *Direito do Procedimento Administrativo,* vol. 1, 1.ª edição, Almedina, 2019, p. 272. Numa perspetiva mais restrita, identificando a essência do princípio da boa administração com um dever de procura por soluções passíveis de projetar uma relação ótima entre recursos mobilizados e resultados pretendidos, cfr. Gonçalves, Pedro, *Manual de Direito Administrativo*, Almedina, 2019, p. 404.

39 Defendendo que, no plano organizatório, o princípio da boa administração se assume como uma norma de natureza "eminentemente programática", na medida em que a sua concretização depende, primacialmente, do legislador, que não está vinculado pelo CPA", cfr. Aroso de Almeida, Mário, *Teoria Geral do Direito Administrativo*, 6.ª edição, Almedina, 2020, pp. 129-130.

40 Cfr. Raimundo, Miguel Assis, "Os princípios no CPA e o princípio da boa administração, em particular", in *Comentários ao Código do Procedimento Administrativo*, vol. I, 5.ª edição, AAFDL editora, 2020, p. 318. No mesmo sentido, cfr. Freitas do Amaral, Diogo, *Curso de Direito Administrativo*, vol. II, 4.ª edição, Almedina, 2020, p. 36.

Tudo, note-se, consequência da imposição constitucional de que o processamento da atividade administrativa garanta "a racionalização dos meios a utilizar pelos serviços"[41]. Mas também dos princípios da *desburocratização* e da *aproximação dos serviços das populações* que a Lei Fundamental da República expressamente acolhe no n.º 1 do seu art. 267.º[42].

2.3 O princípio da Administração Eletrónica

Dito isto, não será excessivo afirmar que a incorporação de novas tecnologias de informação e comunicação na ação administrativa se demonstra incontornável. É que, goste-se ou não, a verdade é que, no mundo de hoje, a consagração de uma *Administração Eletrónica* apresenta-se como uma condição por demais necessária para a plena concretização de todos os princípios constitucionais e legais a que anteriormente fizemos referência.

De resto, tal entendimento surge confirmado pelo n.º 1 do art. 14.º do Código do Procedimento Administrativo; preceito nos termos do qual se estabelece que "os órgãos e serviços da Administração Pública devem utilizar *meios eletrónicos* no desempenho da sua atividade, de modo a promover a *eficiência* (...) e a *proximidade com os interessados*"[43].

Ainda que assim não fosse, porém, a conclusão a forjar dificilmente poderia ser diversa. Afinal, muitos são os exemplos suscetíveis de ilustrar como o progresso da ciência e da técnica pode ser explorado pelas autoridades administrativas, a fim de promover uma melhor realização dos interesses

41 Cfr. o n.º 5, do art. 267.º da Constituição da República Portuguesa. Argumentando que a "ideia fundamental" que o princípio da boa administração incorpora se recorta deste preceito, cfr. Gonçalves, Pedro, *Manual de Direito Administrativo*, Almedina, 2019, p. 401.

42 Assim ressalta, de forma direta, do próprio Preâmbulo do Código do Procedimento Administrativo, onde se esclarece, no §5, que "integram-se nesse princípio [leia-se, o princípio da boa administração] os princípios constitucionais da eficiência, da aproximação dos serviços das populações e da desburocratização".

43 Na sua formulação completa, o preceito em questão dispõe que "os órgãos e serviços da Administração Pública devem utilizar meios eletrónicos no desempenho da sua atividade, de modo a promover a eficiência e a transparência administrativas e a proximidade com os interessados". Todavia, optamos por não fazer alusão à dimensão da promoção de transparência que este preceito encerra: não porque não lhe reconheçamos importância, mas antes, por uma questão de mera objetividade e simplicidade argumentativa. O que se pretende, é pois, não desviar o leitor do foco da nossa análise: a relação entre Administração Eletrónica, eficiência e proteção de dados pessoais; problema cuja complexidade reclama atenção exclusiva.

públicos (secundários) colocados pelo legislador a seu cargo.

Pense-se, nomeadamente, nos benefícios associados à desmaterialização de processos[44]; fenómeno que, tornando a informação interno-administrativa facilmente pesquisável e disponível à distância de um clique[45], permite "uma gestão e um intercâmbio documental permanentes"[46], agilizando o procedimento[47], e, em certos casos, abrindo até porta à redução da despesa pública, por via da redução do pessoal requerido para a execução de tarefas suscetíveis de ser levadas a cabo de forma totalmente automatizada[48]. Ou ainda, nas vantagens decorrentes da disponibilização de serviços administrativos online, o que permite não só quebrar barreiras espácio-temporais entre Administração e Particulares[49], como também garantir a continuidade na

44 Benefícios esses que aparentam ser inequivocamente reconhecidos pelo legislador nacional. Veja-se o disposto no n.º 2, do art. 64.º, do Código do Procedimento Administrativo, o qual determina que "o processo administrativo é preferencialmente desmaterializado, através de ferramentas que permitam a inclusão dos documentos que nele são incorporados e impeçam a sua violação e extravio". Já os processos administrativos em papel, passam a assumir natureza excecional, nos termos do artigo 64.º/4 do mesmo diploma.

45 Cfr. Otero, Paulo, *Manual de Direito Administrativo,* vol. I, 2.ª reimpressão da edição de 2013, Almedina, 2016, p. 488.

46 Idem, ibidem.

47 Idem, ibidem.

48 Idem, ibidem. Importa, todavia, referir que a relação entre a informatização da Administração Pública e a redução do pessoal desta última não é automática e linear. Isto porque, como bem denota Miguel Prata Roque, "ainda que a automatização eletrónica permita a dispensa de trabalho manual e, por conseguinte, de recursos humanos não especializados (ex: assistentes técnicos, funcionários encarregues de registos, de arquivo, de comunicações postais, de atendimento público presencial), não pode negligenciar-se que ela também implica a preparação técnica dos funcionários que lidam com esses recursos eletrónicos e informáticos, bem como a contratação de engenheiros, gestores, programadores e técnicos informáticos que devem garantir a fiabilidade permanente e a atualização dos sistemas eletrónicos e informáticos" (cfr. Roque, Miguel Prata, "O Procedimento Administrativo Eletrónico", in *Comentários ao Código do Procedimento Administrativo*, Volume I, 5.ª edição, AAFDL editora, 2020, pp. 599-600, nota 3).

49 Nesse sentido, cfr., por todos, Otero, Paulo, *Manual de Direito Administrativo,* vol. I, 2.ª reimpressão da edição de 2013, Almedina, 2016, pp. 487-488. Em todo o caso, não deixa o autor de alertar para o reverso da medalha de tal realidade. É que, muito embora concorra para a aproximação dos serviços às populações, permitindo a estas últimas poupar tempo e dinheiro em deslocações presenciais aos primeiros, a verdade é que, numa Administração Eletrónica, "os cidadãos deixam de encontrar um rosto, um nome para o seu contacto junto das estruturas administrativas, criando-se um abismo no trato que desumaniza a Administração Pública". Daí que, na sua ótica, "uma Administração personalista" dificilmente possa ser configurável enquanto uma "Administração integral ou predominantemente eletrónica".

prestação daqueles, 24 horas por dia, 7 dias por semana[50].

Não obstante, é justo sublinhar que as potencialidades da Administração Eletrónica se encontram longe de poder considerar-se esgotadas nos supramencionados domínios. Prova disso, são as crescentes aplicações práticas que a Doutrina tem vindo a projetar para tecnologias como o *Big Data*, a Computação na Nuvem, a Internet das Coisas, a Inteligência Artificial ou a *Blockchain*, no âmbito da função jurídico-administrativa[51]. Aplicações essas que, vão desde a construção de cidades cada vez mais inteligentes (*v.g.*, em planos como a mobilidade, a gestão de resíduos ou a eficiência energética)[52] até à oferta de serviços públicos personalizados, adaptados às reais necessidades de cada indivíduo[53].

Isto, claro está, para nem sequer aludir a situações de excecionalidade, tais como a que hodiernamente vivemos, fruto da situação de emergência sanitária provocada pelo vírus SARS-COV-2 e pela doença COVID-19. Circunstância onde, sem o recurso a ferramentas como portais na Internet, clientes de e-mail ou plataformas de tele e videoconferência, o regular desempenho da atividade administrativa se afiguraria pura e simplesmente impossível, colocando em causa o *princípio da prossecução do interesse público* e, por arrasto, a própria efetivação de uma série de direitos económicos, sociais e culturais da mais reconhecida importância para a generalidade dos membros da coletividade.

---

50 Cfr. Otero, Paulo, *Manual de Direito Administrativo,* vol. I, 2.ª reimpressão da edição de 2013, Almedina, 2016, pp. 487-488; Sarmento e Castro, Catarina, "O Código do Procedimento Administrativo e a Constituição", in *Comentários ao Código do Procedimento Administrativo*, Volume I, 5.ª edição, 2020, pp. 76-77; Dias, José Eduardo Figueiredo / Oliveira, Fernanda Paula, *Noções Fundamentais de Direito Administrativo,* 5.ª edição (reimpressão), Almedina, 2021, p. 106.

51 Para uma breve introdução ao tema, cfr. Agencia Española de Protección de Datos, "Tecnologías y Protección de Datos en las AA.PP.", Novembro de 2020, pp. 2 e ss.

52 Para mais desenvolvimentos, cfr., entre outros, Gutiérrez, Martínez, "Ciudades inteligentes y derecho: de la e-administración a la ciudad inteligente", in *Sociedad Digital y Derecho*, Imprensa Nacional del Boletín Oficial del Estado, pp. 906-907; Calle, Sanchez, "Smart Cities y derechos fundamentales", *European Review of Digital Administration & Law*, vol. 2, n.º 1, 2021, p. 141.

53 Evidenciando os potenciais benefícios associados à implementação deste tipo de serviços, em setores como a Saúde e a Educação, cfr. Ministerio de Ciencia, Innovación y Universidades, "Estrategia Española de I+D+I em Inteligencia Artificial", 2019, pp. 29 e ss.

3. Administração Pública (Eletrónica) e Proteção de Dados Pessoais

3.1 O princípio do respeito pelos direitos e interesses legalmente protegidos dos cidadãos

Sem prejuízo do que precede, importa, todavia, ter presente que a transformação digital da Administração Pública não constitui um processo isento de perigos e/ou inconvenientes[54].

E é assim – não só, mas desde logo[55] – porque a utilização de novos meios (tecnológicos), por parte de órgãos e entes administrativos, no exercício das respetivas funções, pressupõe um incremento do volume de dados pessoais recolhidos, conservados e, enfim, tratados[56], por estas estruturas, de forma *total ou parcialmente automatizada*[57]. O que, naturalmente, faz exponenciar o receio de potenciais *violações de dados pessoais*[58], suscetíveis de causar a cada

54 Para uma síntese, cfr. Otero, Paulo, *Manual de Direito Administrativo,* vol. I, 2.ª reimpressão da edição de 2013, Almedina, 2016, pp. 488 e segs.

55 Mais uma vez – e à semelhança do que fizemos na secção 1.3. do presente texto – alertarmos para o facto de os riscos da Administração Eletrónica não se esgotarem no domínio a que nos dedicaremos ao longo das próximas páginas – leia-se, o da proteção de dados pessoais. É que, para além do que se referirá de seguida, a digitalização da ação administrativa coloca ainda uma série de problemas adicionais, nomeadamente, do ponto de vista (i) da *desigualdade entre cidadãos* (suscitada pela insuficiência de competências técnicas e/ou de recursos financeiros, manifestada por determinados grupos sociais, para a aquisição e manejamento de equipamentos e plataformas informáticas) e (ii) da *cibersegurança de infraestruturas críticas* (cuja excessiva dependência de controlos digitais pode conduzir a efeitos perversos, nomeadamente, em casos de incidentes como ataques de *ransomware*, passíveis de afetar o seu regular funcionamento).

56 Na verdade, a própria recolha e conservação de dados subsumem-se ao conceito de "tratamento", definido no n.º 1, do art. 4.º, do Regulamento Geral sobre a Proteção de Dados como "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados". De todo o modo, optamos aqui por individualizar as referidas operações, empregando o termo "tratar" em sentido estrito, enquanto sinónimo de "processar", por forma a conferir uma imagem mais nítida do problema em causa.

57 Para este facto já advertimos in Alves, Joel A. / Fonseca, Isabel Celeste M., "Legal developments on Smart Public Governance and Fundamental Rights in the Digital Age", in *Legal Developments on Cybersecurity and Related Fields*, Springer (no prelo).

58 Recorde-se que o n.º 12, do art. 4.º do Regulamento Geral sobre a Proteção de Dados define "violação de dados pessoais" como uma "violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".

cidadão prejuízos tão sérios "como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa"[59].

É certo que, em bom rigor, os riscos relacionados com o tratamento de informações de carácter pessoal pela Administração Pública sempre existiram[60], e sempre encerraram um potencial lesivo adicional, relativamente às operações homólogas, desenvolvidas pela generalidade dos operadores privados[61]: fosse pela quantidade de titulares de dados pessoais em jogo[62]; fosse pela sensibilidade e extensão das informações envolvidas[63]; fosse, ainda, pelo tendencial desequilíbrio de forças existente entre Administração e particulares[64].

Sem embargo, ponto é que a Administração Eletrónica veio conferir uma renovada importância a tal problema: em primeiro lugar, por elevar as capacidades de armazenamento da informação administrativa a níveis praticamente ilimitados[65]; em segundo lugar, por tornar mais cómoda, fácil e rápida a realização de outras operações sobre essa mesma informação[66];

59 Cfr. o considerando 85 do Regulamento Geral sobre a Proteção de Dados.

60 Sustentando que a proteção de dados pessoais não é um problema específico da Administração Eletrónica, mas antes da atividade administrativa na sua globalidade, cfr. Maurer, Hartmut, *Derecho administrativo alemán* (tradução espanhola), 1.ª edição, Universidad Nacional Autónoma de México, 2012, p. 457.

61 Cfr. Agencia Española de Protección de Datos, "Tecnologías y Protección de Datos en las AA.PP.", Novembro de 2020, p. 8.

62 Idem, ibidem.

63 Idem, ibidem.

64 Idem, ibidem. A existência de um "desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento", nos casos em que este último seja "uma autoridade pública", é, aliás, expressamente sublinhada no considerando 43 do Regulamento Geral sobre a Proteção de Dados, a propósito do esclarecimento sobre as condições mínimas necessárias para que um consentimento se possa considerar dado de livre vontade, e, como tal, constituir um fundamento jurídico válido para o tratamento de dados pessoais, nos termos do art. 6.º do Regulamento.

65 Cfr. Maurer, Hartmut, *Derecho administrativo alemán* (tradução espanhola), 1.ª edição, Universidad Nacional Autónoma de México, 2012, p. 457.

66 Nesse sentido, sublinhando que "a quantidade, a rapidez e a capacidade de processar e conectar os dados pessoais informatizados ao hoje ao dispor da nova Administração [Eletrónica] nada tem que ver com o modelo clássico da Administração do pré-digital", cfr.

e em terceiro lugar, por levar inclusivamente à aquisição de dados pessoais insuscetíveis de ser obtidos no panorama da Administração do pré-digital[67].

Sempre se dirá – como, aliás, vimos – que os órgãos e entes administrativos se demonstram juridicamente vinculados a *prosseguir o interesse público*; razão pela qual, a probabilidade de ocorrência dos riscos acima referidos se afigure, na verdade, bastante baixa.

Acontece que, conquanto todas as atividades de tratamento de dados pessoais levadas a cabo pela Administração se presumam orientadas por um "espírito de serviço público"[68], tal não significa que não possa haver lugar a desvios[69], nomeadamente, no caso de eventuais ruturas do Estado de Direito[70]; situações de emergência fora do controlo[71]; episódios de corrupção e/ou de abuso de poder envolvendo funcionários públicos[72]; etc. Para além do mais, a realidade tem provado que mesmo tratamentos de dados pessoais leais e lícitos podem redundar em *databreaches* – seja por negligência do próprio responsável pelo tratamento[73], seja devido a ações dolosas, perpetradas por terceiros mal intencionados[74].

Otero, Paulo, *Manual de Direito Administrativo,* vol. I, 2.ª reimpressão da edição de 2013, Almedina, 2016, pp. 491-492, nota 1643.

67 Um bom exemplo disso, prende-se com os dados recolhidos em sítios web e/ou aplicações móveis através da utilização de testemunhos de conexão (*cookies*) e de outras tecnologias de seguimento semelhantes.

68 Cfr. Agencia Española de Protección de Datos, "Tecnologías y Protección de Datos en las AA.PP.", Novembro de 2020, p. 8.

69 Idem, ibidem.

70 Idem, ibidem.

71 Idem, ibidem.

72 Idem, ibidem.

73 Veja-se o que recentemente sucedeu na Noruega, onde a combinação dos sistemas informáticos utilizados por dois municípios recém-agregados – a saber, o Município de Moss e o Município de Rygge – levou, entre outras falhas, a que fossem incorretamente registados os dados relativos à vacinação de inúmeros cidadãos. Para mais desenvolvimentos, cfr. Datatilsynet, "Moss Municipal Council fined", Julho de 2021, disponível em: <https://www.datatilsynet.no/en/news/2021/moss-municipal-council-fined/>

74 Atente-se, a título ilustrativo, ao que ocorreu com a *Transavia*, onde um *hacker* conseguiu penetrar nos respetivos sistemas e obter acesso não autorizado aos dados pessoais de sensivelmente 83,000 clientes. Dados pessoais esses, que haviam sido originariamente recolhidos e ulteriormente tratados pela companhia aérea de forma totalmente legítima. Sobre o incidente em questão, cfr. Autoriteit Persoonsgegevens, "Dutch DPA fines Transavia for poor personal data security", Novembro de 2021, disponível em: <https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fines-transavia-poor-personal-data-security>

Nesta senda, inevitável se torna recordar que, à luz de uma conceção personalista da Administração Pública[75], tal como a acolhida na Constituição da República Portuguesa[76], a (eficiente e eficaz) satisfação das necessidades coletivas não pode ser encarada como um objetivo a atingir a qualquer custo, à semelhança do que ocorre nos sistemas de matriz totalitária[77].

De facto, a Lei Fundamental é clara: "Portugal é uma República soberana, baseada na dignidade da pessoa humana" (art. 1.º); e, ainda, "um Estado de direito democrático baseado na (...) garantia de efetivação dos direitos e liberdades fundamentais" (art. 2.º). Daí que, o interesse público deva forçosamente ser prosseguido, pelos órgãos e agentes administrativos, "no respeito pelos direitos e interesses legalmente protegidos dos cidadãos" (*princípio do respeito pelos direitos e interesses legalmente protegidos dos cidadãos*)[78].

3.2 O princípio da proteção dos dados pessoais

Desta feita, vale a pena enfatizar que a proteção das pessoas singulares relativamente ao tratamento dos dados pessoais que lhes digam respeito é um direito fundamental, expressamente previsto no art. 8.º da Carta dos Direitos Fundamentais da União Europeia, bem assim como no art. 16.º do Tratado sobre o Funcionamento da União Europeia. Sendo que – muito embora de forma algo camuflada[79] – também a Constituição da República Portuguesa "consagra a proteção dos cidadãos perante o tratamento de dados pessoais informatizados"[80], sujeitando-a ao regime específico dos direitos, liberdades

75 Para mais desenvolvimentos, cfr., por todos, OTERO, Paulo, Manual de Direito Administrativo, vol. I, 2.ª reimpressão da edição de 2013, Almedina, 2016, pp. 309 e ss.

76 Cfr. Otero, Paulo, *Direito do Procedimento Administrativo,* vol. 1, 1.ª edição, Almedina, 2019, p. 161.

77 Cfr. Otero, Paulo, *Manual de Direito Administrativo,* vol. I, 2.ª reimpressão da edição de 2013, Almedina, 2016, p. 305.

78 Cfr. a 2.ª parte, do n.º 1, do art. 266.º da Constituição da República Portuguesa, bem como a 2.ª parte, do art. 4.º, do Código do Procedimento Administrativo.

79 Nesse sentido, cfr. Canotilho, José Joaquim Gomes / Moreira, Vital, *Constituição da República Portuguesa Anotada,* vol. I, 4.ª edição, Coimbra editora, 2010, p. 550.

80 Idem, ibidem. Em todo o caso, ponto é que tal proteção não se esgota neste domínio, mas antes se estende, igualmente, "aos dados pessoais constantes de ficheiros manuais" (cfr. o n.º 7 do art. 35.º da Lei Fundamental).

e garantias[81].

E o mesmo se diga da Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais; tratado internacional que, a despeito de não acolher o direito à proteção de dados pessoais, do ponto de vista formal, nem por isso lhe deixa de conferir tutela indireta, em diversas situações, a partir do direito ao respeito pela vida privada e familiar[82].

Acresce que – conquanto tal já fosse, por si só, suficiente[83] – dispõe ainda o art. 18.º do Código do Procedimento Administrativo que "os particulares têm direito à proteção dos seus dados pessoais e à segurança e integridade dos suportes, sistemas e aplicações utilizados para o efeito, nos termos da lei" (*princípio da proteção dos dados pessoais*). Circunstância, que não deixa margem para dúvidas no que respeita à necessidade de os órgãos e agentes administrativos levarem em conta, no desenvolvimento da sua atividade, as posições jurídicas subjetivas reconhecidas a cada cidadão, enquanto titulares de dados pessoais.

4. Epílogo

Do exposto, não parece árduo de compreender que a transição digital constitui um processo especialmente exigente para a Administração Pública, colocando em tensão um conjunto de bens, interesses e/ou valores bastante diversos, mas, ainda assim, identicamente merecedores de tutela, no quadro do nosso ordenamento jurídico-constitucional.

Efetivamente – e tal como procurámos demonstrar ao longo das páginas antecedentes -, a *tecnologificação* da ação administrativa traz

81 Cfr. art. 35.º da Constituição da República Portuguesa, lido em conjugação com o art. 17.º do mesmo diploma.

82 Para mais desenvolvimentos, cfr., com especial interesse, De Hert, Paul / Gutwirth, Serge, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", in *Reinventing Data Protection?*, Springer, 2009, pp. 15 e ss.

83 E é assim, pois que, nos termos do n.º 1 do art. 18.º da Constituição da República Portuguesa, lido em conjugação com os arts. 16.º e 17.º do mesmo diploma, a Administração Pública encontra-se vinculada, enquanto poder público, pelos preceitos constitucionais respeitantes aos direitos, liberdades e garantias, bem assim como por quaisquer outros direitos fundamentais de natureza análoga – incluindo direitos fundamentais fora da Constituição, tais como os constantes de atos legislativos ou de normas de direito internacional.

tanto de *oportunidades* como de *riscos*. Razão pela qual, a mesma possa simultaneamente ser perspetivada, ora como um *meio para uma mais eficiente e eficaz satisfação das necessidades coletivas* – na esteira do que os princípios da *prossecução do interesse público*, da *boa administração* e da *administração eletrónica* determinam –, ora como uma *ameaça para a proteção das pessoas relativamente ao tratamento dos dados de carácter pessoal que lhes digam respeito* – algo que os princípios do *respeito pelos direitos e interesses legalmente protegidos dos cidadãos* e da *proteção dos dados pessoais* visam, num plano contrário, evitar.

Nestes termos – e por forma a solucionar o dilema que serviu de mote à redação do presente estudo[84] – cumpre tomar como ponto de partida as lições de Paulo Otero, segundo as quais, "num cenário crescente de normatividade principialista", os órgãos e agentes administrativos não podem nortear-se por "uma lógica de tudo ou nada, própria da aplicação de regras"[85]. Pelo contrário: a moderna Administração Pública deve comportar-se como uma verdadeira "Administração de balanceamento ou da ponderação"[86], suscetível de contrapesar as diferentes realidades jurídicas conflituantes em cada momento e assegurar "um equilibrar equitativo do [seu] peso relativo"[87]. Donde, a renovada importância do *princípio da proporcionalidade* (ou *da proibição do excesso*) na sua tripla vertente de *adequação*, *necessidade* e *proporcionalidade (em sentido estrito)*[88]/[89].

---

84 Recordando-o: "como aproveitar o progresso da ciência e da técnica, de modo a melhor satisfazer as necessidades da coletividade, sem com isso diminuir a proteção conferida a cada um dos seus membros, contra o tratamento indevido de informações de carácter pessoal que lhes digam respeito? Dito de outro modo, numa versão renovada de um dos mais intrincados desafios a que o Direito Administrativo, desde sempre, procura dar resposta: como compatibilizar as exigências da ação administrativa eletrónica, na prossecução de interesses gerais, com os imperativos de garantias dos particulares, na defesa do seu direito à proteção de dados pessoais?".

85 Cfr. Otero, Paulo, *Direito do Procedimento Administrativo,* vol. I, 1.ª edição, Almedina, 2019, p. 251.

86 Idem, ibidem.

87 Cfr. Otero, Paulo, *Manual de Direito Administrativo,* vol. I, 2.ª reimpressão da edição de 2013, Almedina, 2016, p. 432.

88 Cfr. o n.º 2 do art. 266º da Constituição da República Portuguesa, bem como o art. 7.º do Código do Procedimento Administrativo.

89 Para uma visão aprofundada sobre este princípio e cada uma das subcomponentes

O mesmo é dizer que, a incorporação de quaisquer novos equipamentos ou plataformas tecnológicas, no âmbito da função administrativa, deve ser precedida de uma cuidada reflexão, suscetível de cumulativamente ofertar resposta a três questões essenciais. Primeiro: são os equipamentos ou plataformas em causa aptos, do ponto de vista técnico, para garantir uma (mais) eficiente e eficaz prossecução do interesse público?[90] Segundo: sendo esse o caso, constituem essas ferramentas – ou mais exatamente, a sua utilização, por parte da Administração – uma solução indispensável para a consecução do pré-referido objetivo? Ou existiriam outras alternativas (tecnológicas ou não) equivalentes, menos lesivas ou onerosas para o direito à proteção de dados pessoais dos cidadãos?[91] Terceiro: ainda que se admita que a utilização dos mencionados equipamentos ou plataformas constitui uma medida administrativa *idónea* e *exigível*, face às metas que se pretendem alcançar, é, ainda assim, possível afirmar, com total segurança, que os *benefícios* que daquela se esperam serão superiores aos *custos* que a mesma acarretará? Isto é: pode efetivamente concluir-se pela existência de uma "justa medida" entre as *desvantagens do meios* (para as posições jurídicas subjetivas de cada titular de dados pessoais, isoladamente considerado) e as *vantagens dos fins* (para a coletividade no seu conjunto)?[92]

Assim – e mesmo naquelas situações em que a lei não o imponha de forma explícita –, parece-nos que poderá ser particularmente útil a realização de uma Avaliação de Impacto sobre a Proteção de Dados[93]. Avaliação essa, que

---

que o integram, cfr., por todos, Canotilho, José Joaquim Gomes, *Direito Constitucional e Teoria da Constituição*, 7.ª edição, 14.ª reimpressão, Almedina, 2003, pp. 269 e ss.

90 Idem, p. 269.

91 Idem, p. 270.

92 Idem, p. 270.

93 Recorde-se que o n.º 1 do art. 35.º do Regulamento Geral sobre a Proteção de Dados estabelece, enquanto regime-regra, que deve ser realizada uma Avaliação de Impacto sobre a Proteção de Dados sempre que "um certo tipo de tratamento, *em particular que utilize novas tecnologias* e tendo em conta a sua natureza, âmbito, contexto e finalidades, *for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares*" (sublinhado nosso). Sendo que, mais clarifica o n.º 3 do art. 35.º do mesmo diploma, que uma Avaliação de Impacto sobre a Proteção de Dados será obrigatória, nomeadamente, quando esteja em causa: (i) a avaliação sistemática e completa de aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, na medida em que aquela determine a adoção de decisões que produzam efeitos jurídicos relativamente aos titulares dos dados ou os afetem significativamente de forma similar; (ii) operações de tratamento em grande

permitirá, desde logo: (i) conhecer as operações de tratamento de dados pessoais previsivelmente acopladas ao funcionamento dos referidos equipamentos e plataformas, bem assim como os seus respetivos contornos (tipo de dados envolvidos; volume de titulares afetados; finalidades do tratamento; etc.)[94]; (ii) avaliar a conformidade dessas operações com os princípios e regras decorrentes da pertinente legislação aplicável em matéria de proteção de dados pessoais[95]; (iii) antever os potenciais riscos que tais operações poderão comportar para os direitos e liberdades fundamentais dos titulares dos dados[96]; e (iv) implementar medidas técnicas e organizativas passíveis de fazer frente a esses mesmos riscos[97], reduzindo-os a um patamar considerado aceitável, tendo em conta os objetivos de interesses geral prosseguidos[98].

Por outro lado – e atenta a complexidade da temática em jogo, cujo teor apela a uma contínua (e nem sempre fácil) articulação entre o Direito e as Ciências Tecnológicas[99] – afigura-se-nos igualmente decisivo que as autoridades administrativas cumpram com a sua obrigação de designar um

---

escala, envolvendo dados pessoais pertencentes a categorias especiais previstas no n.º1 do art. 9.º do Regulamento, ou dados pessoais relacionados com condenações penais e infrações ou com medidas de segurança conexas, nos termos do seu art. 10.º; ou (iii) o controlo sistemático de zonas acessíveis ao público em grande escala. Como quer que seja, teve já o recém-extinto Grupo do Trabalho do Artigo 29.º para a Proteção de Dados oportunidade de argumentar – no quadro de Orientações, de resto, acolhidas pelo seu sucedâneo; leia-se, o Comité Europeu para a Proteção de Dados – que nos casos em que não é claro se a realização de uma Avaliação de Impacto sobre a Proteção de Dados é necessária, deve, ainda assim, a mesma ser levada a cabo, uma vez que esta constitui "um instrumento útil para ajudar os responsáveis pelo tratamento a cumprir a legislação relativa à proteção de dados". Cfr. Grupo do Trabalho do Artigo 29.º para a Proteção de Dados, "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679", Outubro de 2017, p. 9, disponível em: <https://www.cnpd.pt/media/f0ide5i0/aipd_wp248rev-01_pt.pdf.>

94 Cfr. a alínea a) do n.º 7 do art. 35.º do Regulamento Geral sobre a Proteção de Dados.

95 Para uma introdução ao tema, cfr. Alves, Joel A., *O novo modelo de proteção de dados pessoais europeu: da heterorregulação à autorregulação publicamente regulada*, Almedina, 2021, pp. 56 e ss.

96 Cfr. a alínea c) do n.º 7 do art. 35.º do Regulamento Geral sobre a Proteção de Dados.

97 Cfr. a alínea d) do n.º 7 do art. 35.º*)* do Regulamento Geral sobre a Proteção de Dados.

98 Não sendo isso, possível, determina o n.º 1 do art. 36.º do Regulamento Geral sobre a Proteção de Dados que o responsável pelo tratamento deve a respetiva autoridade de controlo, antes de proceder ao tratamento.

99 Nesse sentido, cfr. Calvão, Filipa Urbano, *Direito da Proteção de Dados Pessoais. Relatório sobre o programa, os conteúdos e os métodos de Ensino da disciplina*, Universidade Católica Editora – Porto, 2018, p. 14.

Encarregado para a Proteção de Dados[100], o qual deve ser: (i) envolvido, de forma adequada e em tempo útil, em todas as iniciativas de transformação digital que possam impactar na proteção dos cidadãos relativamente ao tratamento de dados pessoais[101]; (ii) munido dos recursos necessários para o exercício das suas funções[102]; e (iii) coberto por adequadas garantias de autonomia e independência[103]. De outro modo, a adoção de soluções (jurídicas e tecnológicas) de cariz compromissório, capazes de atingir o desejável "ótimo de Pareto"[104] entre a realização do bem comum e o respeito pela dignidade inerente a cada indivíduo, enquanto pessoa, dificilmente será concretizável.

100 Nos termos da alínea a) do n.º 1 do art. 37.º do Regulamento Geral sobre a Proteção de Dados, a designação de um Encarregado da Proteção de Dados é obrigatória sempre o tratamento de dados pessoais seja efetuado por uma autoridade ou um organismo público, com exceção dos tribunais no exercício da sua função jurisdicional.

101 Cfr. n.º 1 do art. 38.º do Regulamento Geral sobre a Proteção de Dados.

102 Cfr. n.º 2 do art. 38.º do Regulamento Geral sobre a Proteção de Dados.

103 Cfr. n.º 3 do art. 38.º do Regulamento Geral sobre a Proteção de Dados.

104 Trata-se este de um conceito recorrentemente utilizado no domínio da Economia Política e das Finanças Públicas, para representar aquilo que se idealiza como uma afetação eficiente de recursos, isto é, uma situação "em que é impossível que pelo menos um agente económico fique melhor, sem que o outro fique pior". Para maiores afloramentos, cfr. Pereira, Paulo Trigo et al., *Economia e Finanças Públicas*, 4.ª edição, Escolar Editora, 2012, pp. 44 e ss.

The International Data Transfer Framework and its Political Consequences: a Practical Approach

DIOGO BRITO FONSECA[*]
INÊS PEREIRA AIRES[*]
ISABEL CHOWDHURY[*]
MARGARIDA PERES PEREIRA[*]

Abstract: The international data transfer framework presents itself with many shortcomings. This paper is aimed at analysing European law and determining the practical approach of the courts. It begins by mapping out the troubles of information circulation and legal basis for the regime. There are three paradigmatic cases analysed, *Schrems I* and *II* and *El Gizouli v SSHD*, regarding the European data transfers to the United States and its expected future repercussions in the law. A final recent case, regarding the Lisbon Municipality and Russian Embassy to Portugal, is used to analyse the practice of data protection by state authorities.

Keywords: *Data transfer; General Data Protection Regulation (GDPR); Police directive; Schrems.*

---

[*] Licenciado em Direito e Pós-graduado em Direito da Proteção de Dados pela Faculdade de Direito da Universidade de Lisboa. Frequenta o Mestrado em Direito - Especialização em Direito Empresarial e Tecnologia na NOVA School do Law.

[*] Advogada-estagiária. Licenciada em Direito e Pós-graduada em Direito da Proteção de Dados pela Faculdade de Direito da Universidade de Lisboa. Frequenta o Mestrado em Direito -Especialização em Direito Empresarial e Tecnologia na NOVA School do Law.

[*] Consultora jurídica. Licenciada em Direito pela Faculdade de Direito da Universidade de Lisboa. Frequenta o Mestrado em Direito - Especialização em Direito Empresarial e Tecnologia na NOVA School do Law.

[*] Licenciada em Direito pela Faculdade de Direito da Universidade de Lisboa. Frequenta o Mestrado em Direito - Especialização em Direito Empresarial e Tecnologia na NOVA School do Law.

Resumo: O regime da transferência de dados internacional apresenta várias lacunas. Este texto visa descortinar o Direito Europeu e a demarcação da abordagem prática dos tribunais. Mapeia as dificuldades da circulação de informação e a base legal do regime. Revê-se três casos paradigmáticos: *Schrems I* e *II*, e *El Gizouli v SSHD*, como exemplos de transferência de dados europeus para os E.U.A., e as repercussões esperadas na lei. Analisa-se ainda o caso da transferência de dados entre o Município de Lisboa e a embaixada da Rússia em Portugal para averiguar o rigor da proteção de dados pelas autoridades governamentais.

Palavras-Chave: *Transferência de dados; Regulamento Geral sobre a Proteção de Dados (RGPD); Diretiva de Polícia; Schrems.*

1. Introduction

The digital economy[1] has pushed data flows into an unprecedented and large scale level, generating a whole industry around it, the data industry, aided by the way the internet has globalised trade. Practically every website we visit on a daily basis asks for data in exchange for their content, through cookies,[2] making them effective intermediaries in the data trade, and allowing them to continue to live by selling that data to interested parties or using it for their own benefit. The truth is: our current digital footprint contains almost every digitalizable aspect of our lives. It is extremely difficult, if not almost

1 "The digital economy is the economic activity that results from billions of everyday online connections among people, businesses, devices, data, and processes. The backbone of the digital economy is hyperconnectivity which means growing interconnectedness of people, organizations, and machines that results from the Internet, mobile technology and the internet of things (IoT)", in *What is digital economy?*, Deloitte. Available at: <https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html>

2 "Cookies are small files that websites send to your device that the sites then use to monitor you and remember certain information about you — like what's in your shopping cart on an e-commerce site, or your login information. These pop-up cookie notices all over the internet are well-meaning and supposed to promote transparency about your online privacy." in STEWART, Emily, *Why every website wants you to accept its cookies*, Vox, 2019. Available at: <https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy>

impossible for a person to live a normal life without leaving a digital footprint. And this is where concerns rise: around the possible malicious and legally dubious purposes data about these individual, private citizens may be used.

The GDPR states as the reasoning behind its conception the protection of natural persons, under article 8(1) of the Charter of Fundamental Rights of the European Union

(EUCFR) and article 16(1) of the TFEU, and the particular conditions of increased cross-border data flows due to the creation of the EU internal market. With its creation in 2016, it is now the leading data protection framework in the world and has inspired many other countries to adopt similar ones.[3]

Given the context we previously mentioned, it is natural that data management is needed, especially when data is being exchanged between two legal orders that offer the data subject different levels of protection. The legal regime for data transfers is defined in articles 44 and following. This part of the GDPR assumes particular relevance due to the importance and goal the EU has set as to protecting natural persons as much as possible within its jurisdiction. This is reflected in the adequacy decision criteria denounced in article 45, allowing data transfers to proceed only when the third country in the negotiation is deemed to have a data protection framework that "ensures an adequate level of protection".[4]

In this context, and throughout this paper, we wish to explore the complexities and vicissitudes of this framework. We will focus on the practical application it has, how it influenced politics, was used as a tool for political manoeuvring and abuse and reflect the lack of international understanding in a search for a mutual response to data transfer problems.

---

3 Greenleaf, Graham, *Global data privacy laws 2019: 132 national laws & many bills*, 157 Privacy Laws & Business International Report, 14-18, 2019. Available at: <*https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593*>

4 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), Article 45(1)

2. Democracies facing the Information Wars

We live in an age that is driven by information. Technological breakthroughs . . . are changing the face of war and how we prepare for war.
William Perry, 19th US Secretary of Defense

If until nowadays the Government's main concern was external threats, today is cyberspace security and defense. The Portuguese Institute of National Defense defines cyberwar as a "conflict between two or more nations or between different groups within a nation where cyberspace is the battlefield".[5] When related to data, we can talk about "information warfare", meaning any action to deny, exploit, corrupt or destroy the enemy's information and its functions"".[6] The information manipulation problem is universal. Government information management is related to national security and international reputation and, in democracies, where the circulation of information is free, this issue is particularly dangerous. Information is not just an instrument, but a vulnerability source.

2.1 Information warfare

"Information warfare is not a new phenomenon, yet it contains innovative elements as the effect of technological development, which results in information being disseminated faster and on a larger scale".[7] The internet, as an open global resource and international cooperation, has a huge role in society, "enhances and expands the possibilities of data acquisition, information defence, and information disruption, and makes it easy to reach both the citizens of a given country and the international".[8] "Fake news", "disinformation", "propaganda", are all terms used to describe this phenomenon.

---

5 (Free translation)

6 Borden, Col Andrew, *What is Information Warfare?*, USAF, p. 1. Available at: <https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf>

7 Nato, *Media – (Dis)Information – Security*. Available at: <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf>

8 Ibid.

Historically, and according to the US Army Heritage and Education Center[9]information warfare has been achieved with psychological operations and electronic operations. For the purpose of controlling the American propaganda machine, Franklin Roosevelt established the Office of War Information. As an example, around 1943/1945 the Army Air Forces use to make strategic radio transmissions coordinated with the bombing.

The use of information as a weapon, in the context of a political war, has some risks. "Today, the collection, analysis, and sale of personal information powers global economies; information is, as the dictum goes, power, but we can also argue that it acts as a modern-day currency".[10]

We are currently living in an information era, where "technology allows both private companies and public authorities to make use of personal data on an unprecedented scale to pursue their activities".[11] According to the Recital (16) of the GDPR, the Regulation "does not apply to […] activities concerning national security". However, in the current digital economy, the main economic actors are corporations, especially technology companies.

As GDPR mentions, in Chapter V, data protection rules do apply in international data transfers and the supervisory authorities "shall take appropriate steps to […] the protection of personal data and other fundamental rights and freedoms".[12]

2.2 Data transfers

There have been some attempts to prevent data transfer malicious threats, for example, in 2006 the EU launched a Directive that "required the providers of publicly available electronic communications services and networks to retain traffic and location data belonging to individuals or legal entities for up to two years".[13] [14]

9 U.S. Army Heritage and Education Center, *A Return to Information Warfare*

10 Strategy Bridge, *Thucydides in the Data Warfare Era*, 2018. Available at: <https://thestrategybridge.org/the-bridge/2018/5/30/thucydides-in-the-data-warfare-era>

11 GDPR Recital (6)

12 GDPR Article 50

13 Bruegel, *Data transfers under the threat of terrorist attacks*, 2018. Available at: <https://www.b ruegel.org/2015/12/data-transfers-under-the-threat-of-terrorist-attacks/>

14 In April 2014, however, the ECJ concluded that the Directive interferes with the

The recent attacks, together with the Schrems[15] decision, challenge the ability to transfer data. Faced with the manipulation of information, the consequences are now taken seriously, States have taken several measures ranging from organisational design to the regulation of the media, through the role of parliaments and public awareness.[16] The definition of "information manipulation" is not consensual and the difficulty of qualifications leaves room for arbitrariness in determining the illegal nature of some actions. Although there is no common sense on what qualifies as an act of "cyberterrorism", according to the US Federal Bureau of Investigation (FBI), cyberterrorism is the "premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against noncombatant targets by subnational groups or clandestine agents". Cyberterrorism is a powerful tool because "Internet […] provides a global pool of potential recruits and donors. Online terrorist fundraising has become so commonplace that some organizations are able to accept donations via the popular online payment service PayPal."[17]

Regarding data protection, the EU adopted, in 2005, the European Union Counter-Terrorism Strategy that comes down to four principal ways of approach: i. prevention; ii. protection; iii. investigation; iv. post-attack responses. The current EU Counter-Terrorism Strategy belongs to the EU Global Strategy that identifies cyber threats as one of the main threats that the EU is facing.[18] The EU cooperates with international organisations and bodies to develop strategies for these threats. International data transfers are essential to daily business operations.[19] Even though there are many ways to secure the transmission of data, one of the main concerns is related to data collection and

---

fundamental rights of EU citizens and violates the right to protection of personal data.

15 P. 9.

16 Marangé, Céline, QUESSARD, Maud , *Les guerres de l'information à l'ère numérique*, PUF

17 Kaplan, Eben, *Terrorists and the Internet*, Council on Foreign Relations, 2009. Available at: <https:// www.cfr.org/backgrounder/terrorists-and-internet>

18 European Security & Defence, *EU Counter-Terrorism Strategy*, 2020. Available at: <https://euro-sd.com/ 2020/02/articles/16153/eu-counter-terrorism-strategy/>

19 Deloitte, *GDPR Update: The future of international data transfers*. Available at: <https://www2.deloit te.com/ch/en/pages/risk/articles/gdpr-the-future-of-international-data-transfer.html>

use. Data collection is vulnerable to several risks. The device's connectivity leaves data more vulnerable to a breach, and when a data breach takes place, the entire system is at risk of being compromised.[20] Nowadays, over 130 jurisdictions[21] have some form of privacy and data protection legislation and almost one in three companies fall under the EU GDPR jurisdiction.[22] But different jurisdictions have different points of view. "The EU stands firmly for the interests of the individual. […] Europeans must provide positive consent for the ways their data is used, and they have the right to access and erase that data, as well as the "right to be forgotten." In the opposite corner sits the United States and the giant US corporations that trade in personal data for profit, and whose practices have expanded largely unchecked. One ideology puts the control of personal data in the hands of the individual, the other cedes control to the corporation. (A third approach is state control of data, which is emerging as China's social credit system, though that remains as yet an internal policy.) But these differing views about data protection cannot jostle for dominance for much longer. As trade grows increasingly global, it's becoming clear that personal data crosses borders far too easily for contrasting models to co-exist".[23] Understanding the importance of the data and protecting it as an asset in order to manage possible threats has a more positive impact than trying to avoid cyber risk.

States security against cyber attacks must be a priority to the governments. Data as a weapon and data as a goal is a reality. The use of information to manipulate ideas or cyber-attacks whose intention is to steal private and confidential information are a risk to societies. When democracies are the target, these threats have even more impact. Every day huge amounts of data are collected and processed, and the use of this information is great for society, for example, when used in scientific and/or social research. But, as with everything, it also has a "dark side", such as fake news and massive control.

---

20 Hanover, *How Data Collection Impacts Cybersecurity*, 2020. Available at: <https://www.hanrec.com /post/how-data-collection-impacts-cybersecurity>

21 i-Sight, *A Practical Guide to Data Privacy Laws by Country*, 2021. Available at: <https://www.i-sig ht.com/resources/a-practical-guide-to-data-privacy-laws-by-country/>

22 Ibid.

23 Pendergats, Tom*, The Next Cold War Is Here, and It's All About Data*, 2018. Available at: <https://w ww.wired.com/story/opinion-new-data-cold-war/>

One of the typical examples is the governments' elections, where news has an important role in opinion-making and, consequently, in the ballots. Most of the digital infrastructure is managed by the private sector and the development of, for example, surveillance tools are *subsequently used to attack fundamental liberal principles like press freedom*.[24]

Concerning AML/CFT[25] and economic effects of information warfare, since money laundering requires market manipulation[26] and criminal intention, that also causes damages to democracies, especially economically. "AML/CFT controls mitigate the adverse effects […] and promotes integrity and stability".[27]

2.3 Recommendations & suggestions

Since the world is becoming more and more connected, is a global strategy against "unprotected" data transfers, including both States and Corporations concerns and contributions. Regulating without strangling technology improvements must be one of the purposes, as well as public investment in human resources. "In its latest annual Cyber Security Breaches Survey the Government Department for Digital, Culture, Media and Sport (DCMS) reported that cyber security is a high priority for 78% of businesses, up from 74% last year."[28] As Marrietje Schaake said, democratic nations must ensure that the digital ecosystem operates according to democratic values.[29]

Another suggestion**,** and agreeing with James Coker, is the development of stronger transparency requirements.[30] "It is easy to see that information

---

24 Coker, James, *#BHEU: How to Create a Safe and Democratic Digital Infrastructure,* Info Security. Available at: <https://www.infosecurity-magazine.com/news/bheu-safe-democratic-digital/>

25 Anti-Money Laundering/Combating the Financing of Terrorism.

26 International Monetary Fund, *Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)*. Available at: <https://www.imf.org/external/np/leg/amlcft/eng/>

27 Ibid.

28 Hallett, Steve, "How Data Collection Impacts Cybersecurity", in Hanover, 2020. Available at: <https://www.hanrec.com/pos t/how-data-collection-impacts-cybersecurity>

29 Coker, James, "BHEU: How to Create a Safe and Democratic Digital Infrastructure", in Info Security Magazine, 2021. Available at: <https://www.infosecurity-magazine.com/news/bheu-safe-democratic-digit al/>

30 Ibid.

warfare is no less complex than traditional warfare".[31] The transversal nature of this subject/discussion is obvious and one of the concerns is "the opacity that rules over the choices made by the largest platforms, to which neither legislators nor users have access".[32] "Information warfare is all about measures to improve (or degrade) the efficiency of decision-making".

"The maximum theoretical efficiency depends on the amount and quality of data available and the amount of ambiguity in the data".[33] From what we have exposed, the collaboration between democracies is crucial, aligned with company resources and knowledge.

3. The Impact of Schrems I and Schrems II in International Data Transfers

3.1 Legal context

The GDPR, safeguards "any transfer of personal data which are undergoing processing or are intended for processing after transfers to a third country or an international organisation"[34]. The transfers of personal data need to rely on one of the legal basis for transfers provided by the GDPR under Chapter V, but as well as all the rules and principles stated in this regulation.

Under the European Union data protection law, three mechanisms allow for personal data to be transferred from a Member State to a third state: (1) transfers can be based on a Commission decision finding that the third state ensures an "adequate level of protection"[35]; (2) in the absence of the prior point, the transfer can take place when it is accompanied by "appropriate safeguards"[36], like Standard Contractual Clauses, SCCs, or Binding Corporate

31 Burns, Megan, "Information Warfare: What and How?", 1999. Available at: <http://www.cs.cmu.edu/~./burnsm/InfoWarfare.html>

32 Marangé, Céline, Quessard, Maud, "Les guerres de l'information à l'ère numérique", PUF, 2021

33 Borden, Andrew, "What is Information Warfare?", USAF, p. 5. Available at: <https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf>

34 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, article 44. Available at: <Art. 44 GDPR – General principle for transfers - General Data Protection Regulation (GDPR) (gdpr-info.eu)>

35 Article 45 of the General Data Protection Regulation, GDPR

36 Article 46 GDPR.

Rules, BCRs[37]; and lacking this safeguards, based on certain derogations for specific situations[38].

Many of the most interesting cases in privacy from the last few years have dealt with international data transfers, such as the *CompuServe*[39], the *Lindqvist*[40], the *Passenger Name Record*[41] cases, and even the *Microsoft Warrant*[42] case. As different as those cases might be, they all assumed that there is an established system of how transfers of personal data can be done legally[43], but that understanding was challenged by the Court of Justice of the European Union with the *Schrems*[44] case, arising from Edward Snowden's revelations that the National Security Agency had been operating secret surveillance programmes, which brought the beginning of a development where all the mechanisms for international data transfer are scrutinised in much more detail but also more protective of the specific data carried in the process.

---

37 Article 47 GDPR.

38 Article 49 GDPR.

39 *Compuserve* (1998) 8340 Ds 465 Js 173158/95 (AG München); *Compuserve* (1999) 20 Ns 465 Js 173158/95 (LG München). The case dealt with the liability of the German chairman of the access provider CompuServe for illegal content accessible via the intranet. Available at: <https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=AG%20M%FCnchen&Datum=28.05.1998&Aktenzeichen=8340%20Ds%20465%20Js%20173158/95>

40 Reference to the Court under Article 234 EC by the Göta hovrätt (Sweden) for a preliminary ruling in the criminal proceedings before that court against Bodil Lindqvist, Case C-101/01 Lindqvist [2003] ECR I-12971. Clarified the meaning of the provisions relating to transfers of personal data to third countries or international organisations. Available at: <https://curia.europa.eu/ju ris/liste.jsf?num=C-101/01>

41 Joined Cases C-317/04 and C-318/04 *European Parliament v Council of the European Union (Passenger Name Record)* [2006] ECR I-04721; Opinion 1/15 *Concerning the request for an opinion by the European Parliament regarding the agreement envisaged between Canada and the European Union on the transfer of passenger name record data*. Available at: <https://curia.europa.eu/juris/liste.jsf?num= C-317/04&language=en>

42 United States District Court, E.D., Pennsylvania, *Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 2017, 232 F. Supp. 3d 708 (E.D. Pa. 2017). Available at: <https://casetext.com/case/in-re-search-warrant-no-16-1061-m-to-google>

43 Bräutigam, Tobias, "The Land of Confusion: International Data Transfers between Schrems and the GDPR", 2016). Tobias Bräutigam and Samuli Miettinen (eds), 'Data Protection, Privacy and European Regulation in the Digital Age' (Helsinki, 2016), Helsinki Legal Studies Research Paper 46, page 4. Available at SSRN: <https://ssrn.com/abstract=2920181>

44 Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, Request for a preliminary ruling from the High Court (Ireland), Case C-362/14 Schrems v Data Protection Commissioner (Grand Chamber, 6 October 2015). Available at: <https://curia.europa.eu/juris/liste.jsf?num=C-362/14>

3.2 Brief overview of Schrems I case: from the (un)safe harbour to the Privacy Shield

Transatlantic data flows between the European Union and the United States, or US, were made possible in 2000 through the Safe Harbour[45] scheme. The Safe Harbour was based on a system of voluntary self-certification and self-assessment of US-based companies that they abide with certain data protection principles combined with some intervention by the public authorities.[46] In practical terms, it was required to the US companies to register their compliance with the Safe Harbour principles with the United States Department of Commerce, while the Federal Trade Commission was responsible for enforcing the agreement, having the European Commission to decide on the recognition of the adequacy of the protection provided by these principles.

The European Commission, after thirteen years, with the breach of trust caused by the American "widespread surveillance of private communications of citizens, companies or political leaders"[47] to the transfer of personal data from citizens of the European Union to the United States, brought to a decision, two years later, that entailed this processing of personal data beyond what is strictly necessary and proportional to the imperatives of national security protection and took the opportunity to clarify the adequacy criterion[48], *Schrems I*.

Maximilian Schrems, an Austrian lawyer, lodged a complaint asking the Irish Data Protection Commissioner to prohibit Facebook Ireland from

---

45 European Commission Decision of 26 July 2000 pursuant to Directive 95/46 on the level of protection afforded by the "safe harbour" principles and the most frequent questions (Faqs) issued by the Department of Commerce of the United States of America (Decision 2000/520/EC). Available at: <2000/518/CE: Decisão da Comissão, de 26 de Julho de 2000, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção adequado dos dados pessoais na Suíça [notificada com o número C(2000) 2304] (Texto relevante para efeitos do EEE.) - Publications Office of the EU (europa.eu)>

46 Tzanou, Maria, "Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights", page 5, 2020, Available at SSRN: <https://ssrn.com/abstract=3710539>

47 European Commission, Communication from the commission to the European parliament and the council, Rebuilding Trust in EU-US Data Flows, Brussels (27 november 2013), page 2. Available at: <https://eur-lex.europa.eu/resource.html?uri=cellar:4d874331-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF>

48 Tzanou, Maria, page 5, 2020.

transferring his personal data to servers located in the United States,[49] arguing that the law and practice in force in that country, in particular the surveillance activities of intelligence services, did not meet the requirement of the level of adequate protection[50]. The Court of Justice of the European Union issued its decision in 2015, concluding that the United States authorities were able to access the personal data transferred from the European Union Member States and process it beyond the strictly necessary and proportionate to the protection of national security.[51]

So, what was decided, directly, was that the US data privacy regime lacks adequate protection towards the European citizens, due to: (1) the regime including different sources like the US Constitution, the Supreme Court case law, federal legislation, State legislation and the theory of torts;[52] (2) the pure nature of self-regulation, without any *ex ante* or *ex post* of a public authority[53]; (3) "adequate level of protection" shall be interpreted as requiring the third country to effectively ensure a level of protection of fundamental rights and freedoms "substantially equivalent" to within the EU,[54] and we cannot argue that a country that has general derogations which makes possible unjustified and unlimited interference with the fundamental rights of data subjects[55], has the necessary level of protection.

The court clarified that a third country has sufficient protection only if it complies with a specific protection scheme for natural persons about the interference with fundamental rights for the purpose of State surveillance,

---

49 EDPS Case Law Digest: Transfers of personal data to third countries, page 8, 2021, . Available at: <https://edps.europa.eu/data-protection/our-work/publications/court-cases/case-law-digest-2021-transfers-personal-data_en>

50 Moniz, Maria da Graça, "A Extraterritorialidade do Regime Geral de Proteção de Dados Pessoais da União Europeia: Manifestações e Limites", page 258, 2018. Available at: <https://run.unl.pt/bitstream/10362/89180/1/Fonseca_2019.pdf>

51 This discussion can be found in Tzanou, Maria, 'European Union Regulation of Transatlantic Data Transfers and Online Surveillance' (2017) 17(3) Human Rights Law Review 545. Available at: <https://academic.oup.com/hrlr/article-abstract/17/3/545/3061949>

52 Shaffer, Greggory, "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards", 25 Yale Journal of International Law 1, 22, 2000.

53 Moniz, Maria da Graça, 2018.

54 Judgment of the ECJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, (6 October 2015), paragraphs 73 and 74.

55 Judgment of the ECJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, (6 October 2015), paragraphs 87 and 88.

but also showed the lack of legitimacy in inadequate protection against such interference in the several Member States[56] and the lack of guarantee of the protection continuity after the personal data have been transferred to the third country,[57] assuring the fundamental rights and guarantees to which everyone is entitled in the European Union.

It was a "landmark" judgement,[58] but given his, negative financial, impact on the transatlantic trade and the promises made by the US to reform the law and current practises,[59] the European Commission adopted a new decision, known as the Privacy Shield[60] in 2016 to rekindle this connection.

Privacy Shield was adopted to replace Safe Harbour, invalidated in *Schrems I*, in the form of an adequacy decision. It was based on a system of self-certification by which US organisations committed to a set of privacy principles,[61] that included a segment on the access and use of personal data that is transferred under the agreement by the United States public authorities for national security and law enforcement motives. Attached to the draft adequacy decision were seven annexes from US government entities that set out various commitments and requirements, such as increased data subject protections and greater requirements for data controllers to respect data protection principles, including purpose limitations[62], but also strengthening obligations on companies regarding limits on data retention and onward transfers.

---

56 Tzanou, Maria: "The EU's claim as a moral leader in respect for fundamental rights is not always obviousv. "The war against terror and transatlantic information sharing: spillovers of privacy or spillovers of security", UJIEL, n.º 31, vol. 80, (2015), p. 87 e ss..

57 G29, "Working document on a common interpretation of paragraph 1 of Article 26 of Directive 95/46 (25 november 2005). Available at: <https://www.pdpjournals.com/docs/88080.pdf.>

58 Kuner, Christopher, "Reality and Illusion in EU Data Transfer Regulation Post Schrems" (March 2016) Cambridge Faculty of Law Legal Studies Research Paper Series, Paper 14/2016. Available at: <https:// papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346>

59 European Commission, "Transatlantic Data Transfer: Restoring Trust through Solid Guarantees", (29 February 2016), page 17. Available at: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3 A52016DC0117>

60 Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–U.S. Privacy Shield, Brussels, 12 July 2016, C(2016) 4176 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG>

61 Tzanou, Maria, (2020), page 12.

62 European Commission Unveils EU-U.S. Privacy Shield, EUR. COMM'N (29 February 2016). Available at: <https://ec.europa.eu/newsroom/just/items/30375/en>

A lot of elements in the Privacy Shield showed how hard it was to combine the different notions of privacy between the U.S. and Europe[63], from the lack of central supervisory authority in the US, as expected in the article 51. of the GDPR, to the differences facing structural definitions[64]. Even if the Commission found that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the US, serious concerns were raised as to whether Privacy Shield complies with EU data protection and privacy standards,[65] mainly because the decision was based on US assurances, without any major substantive commitments by the respective authorities to comply with European Union fundamental rights requirements as expressed by the Court of Justice of the European Union in Schrems I.

With all of this in mind, it was expected that new problems would arise by the Commission's failure to resolve the structuring issues for data subjects on this matter, the American data surveillance programmes that were signalled, again, by *Max Schrems* on the *Schrems II* case.

3.3 The Schrems II case: additional protective measures and extraterritorial application

Following the invalidation of Safe Harbour, *Max Schrems*, reformulating his complaint lodged with the Irish Data Protection Authority, asked the Data Protection Commission to suspend his personal data held by Facebook Ireland to Facebook, Inc claiming that these could be made available to US authorities, such as the National Security Agency and the Federal Bureau of Investigation, in the context of surveillance programmes that impede the exercise of the rights

63 Bräutigam, Tobias, (2016), page 159.

64 European Commission, "Annexes to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield" C (2016) 4176 final Annexes 1 to 7 (Brussels, 12 July 2016) and Annex II, part II, art. 2 (c)). Regarding the "choice" principles that define the permission level needed to share sensitive data as "affirmative express consent", opt in.

65 See WP29, Opinion 1/2016 of 13 April 2016 on the EU–U.S. Privacy Shield draft adequacy decision WP 238. Available at: <https://www.pdpjournals.com/docs/88536.pdf.>

guaranteed in the Charter of Fundamental Rights of the European Union[66]. The legal framework of the claim this time concerned the data transfers in the U.S. under the Standard Contractual Clauses, SCCs, based on the Decision 2010/87.[67]

On 16 July of 2020, the Court of Justice of the European Union, CJEU, published its *Schrems II*[68] judgement that invalidated the European Commission's Privacy Shield adequacy decision[69]. The court held that the U.S. does not provide a sufficient level of protection, as guaranteed by the GDPR and the EUCFR, having surveillance programmes, such as *PRISM* and *UPSTREAM*, not being limited to the strictly necessary, which results in disproportionate interference with the rights to protection of data and privacy,[70] regarding the lack of actionable rights for European Union subjects against United States authorities and the broader powers conferred upon the U.S. authorities.

Following the Advocate General *Saugmandsgaard Øe's* opinion[71], the court affirmed the validity of the SCC Decision while stipulating stricter requirements for the SCC-based transfers. The Standard Contractual Clauses do not present lawful or unlawful grounds for data transfer, but if the entities seek to transfer data based on this mechanism, they need to ensure that the data subject has a level of protection essentially equivalent to that guaranteed by

66 The articles 7., 8. and 47. of the EUCFR.

67 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ 2010 L 39/5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344/100, 'Decision 2010/87').

68 Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Request for a preliminary ruling from the High Court (Ireland). Available at: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=254046>

69 European Parliament, AT A GLANCE, The CJEU judgment in the Schrems II case (2020). Available at: <https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN .pdf.>

70 Based on article 45(1) of the GDPR and articles 7., 8. and 52.(1) of the EUCFR.

71 Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Request for a preliminary ruling from the High Court (Ireland). Available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX: 62018CC0311>

the GDPR and EUCFR, if necessary, with additional, supplementary, measures to compensate any lacunae in the protection of third-country legal systems,[72] provided that the data exporter concluded that the risks, evaluated by risk assessments[73]access to data by the public authorities of the third country could be addressed by these measures.

Christopher Kuner points out that the CJEU "suggests using 'supplementary measures' to protect data under the SCCs but does not explain what measures these could be".[74] The author affirms that, in effect, all the SCCs become "mini adequacy decisions". In my opinion, this complexity can lead companies, especially smaller ones, to avoid this course entirely, while larger ones will be able to afford the expensive legal advice reviewing a foreign nation's surveillance law for compatibility with EU law, smaller firms will not,[75] making this transfer vehicle too complicated for a process that is responsible for a large fraction of data exports from the European Union[76].

As the CJEU did not define what these additional measures were, the European Data Protection Committee, EDPB, approved Recommendation 1/2020[77], following a public consultation, to guide companies on the scenarios where such measures would be available to exporters to ensure the lawfulness of their international transfers. The EDPB provided a non-exhaustive list of

72 European Parliament, AT A GLANCE, The CJEU judgment in the Schrems II case (2020), page 2. Available at: <https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ ATA(202 0)652073_EN .pdf>

73 Luther., First-aid kit for "Schrems II" compliance (2020). Available at: <https://www.luther-lawfirm.com/f ileadmin/user_upload/OnePager_Erste_Hilfe_Schrems_II_EN.pdf>

74 Kuner, Christopher, The Schrems II judgment of the Court of Justice and the future of data transfer regulation (17 July 2020). Available at: <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/>

75 Chander, Anupam, "Is Data Localization a Solution for Schrems II?", Journal of International Economic Law, Forthcoming, page 5, (July 27, 2020). Available at: <https://ssrn.com/abstract=3662626>

76 The International Association of Privacy Professionals surveyed members and reported that "Seven in 10 respondents say their organization transfers data out of the EU to non-EU countries…. The most popular of these tools — year over year — are overwhelmingly standard contractual contracts: 88% of respondents in this year's survey reported SCCs as their top method for extraterritorial data transfers, followed by compliance with the EU-U.S.Privacy Shield arrangement (60%).").

77 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 (18 June 2021). Available at: <https://edpb.europa.eu /system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf>

supplementary measures, which may add to the safeguards found in article 46 GDPR transfer tools, regarding the technical, contractual, and organisational aspect of it that data exporters need to have in mind regarding the context of the transfer[78], the third country law[79] and the transfer tool used[80].

Generally speaking, the Court's analysis in *Schrems II* is unparalleled for the theoretical interrogations about the US surveillance programmes, and is explained by the fact that a detailed description of US national security and surveillance law was included in the Commission's Privacy Shield adequacy decision. Nevertheless, we can argue that the external dimension of extraterritoriality, examination of the foreign law, was an easier task for the Court with respect to the Privacy Shield than with Safe Harbour, as the former explicitly contained the legal bases regarding US authorities' access to personal data.[81] It is argued that the extraterritorial application of data privacy rights must be based on "rules that are reasonably clear and predictable, both about the threshold question of *applicability* and with regard to the *merits*"[82]. In my opinion, *Schrems II* achieves these requirements, because it establishes the applicability of the European Union data protection law to adequacy decisions for international data flows under the GDPR in the light of the EUCFR, but also this case constructed an applicable test to the external interferences, by interpreting Article 52(1) of the EUCFR in the context. The CJEU recognizes the differences between the internal and external settings by acknowledging minimum guarantees of the data that have been transferred to third countries for the persons to have enforceable rights and sufficient protection of any abuse, and not to require the intelligence files to be reviewed by citizens of another country, like some authors may emphasize[83].

78 EDPB recommendation mentioned above (18 June 2021), page 4.

79 EDPB (2021), page 4.

80 EDPB (2021), page 38.

81 Tzanou, Maria, (2020), page 17.

82 Milanovic, Marko, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" 56 Harvard International Law Journal 81, 132, 2015.

83 Swire, Peter, '"Schrems II" backs the European legal regime into a corner — How can it get out?", International Association of Privacy Professionals (IAPP), 2020. Available at: <https://iapp.org /news/a/schrems-ii-backs-the-european-legal-regime-into-a-corner-how-can-it-get-out/>

Anyhow, although the Court's tried to be flexible in the extraterritorial context and giving solutions, and obligations, to companies and estates to manage international data transfers to European Union countries, there are challenges remaining that make the future of this vital matter uncertain.

3.4 The challenges of Schrems II and the future of "trans-data"

The *Schrems I* case demonstrated that the European Union was not successful in guaranteeing the fundamental right to the protection of personal data nor the adequacy procedure or appropriate safeguards serving no purpose when the data subjects live in an illusion that they are being protected[84] when the personal data is being transferred to third countries where surveillance programmes with not enough safeguards for the ones that are being supervised.

Schrems II was an evolution. It presented a more robust internal, and not that robust, external approach to extraterritoriality bringing legal certainty and clarity of the applicability of EU law and the merits of assessing external interference with EU fundamental rights but also, with the help of EDPB, presented to the relevant parts affected that there are ways to maintain the transatlantic market operating, with risk mitigation from additional protective measures. The achievements that were brought to the case were achieved indirectly with the highlight of something that is not in the article 44. and 45. of the GDPR, the concept of *risk assessment*, a development of the concept of *accountability*, because the entities need to be accountable, responsible, for what they do.

But even if it evolved, it was not the metamorphosis that was necessary, and here is why: the Court opened the discussion of how we can develop the steps to allow us to process data internationally in the future but didn't say that we needed something new compared to the last decision; the GDPR and Directive do not solve the issue in this case, because, even with all the efforts made by the companies that are following the recommendations, third parties are still able to perform these type of things, continuing to be illusory for the data subjects; increased burdens for both data controllers that transfer data and

84 Moniz, Maria da Graça, 2018, page 289 and 290.

the parties in third countries that received them[85]; and also third countries have in place regulation that allows data surveillance and European regulation that *per si* cannot solve this.

Technology can help find solutions, but before we get too inventive, we need to be reminded of the limitations that some emerging ones has, like *Blockchain*. Having the data being stored in a digital ledger that makes it hard to find, affects the rights of data subjects, but we also have a regulatory issue, because companies that have their headquarters in specific countries are forced to collaborate with authorities of their countries, even if they are providers of a technology that ensures that they do not have access to data, by law they are forbidden for having that solution, legal problems that are involved in this can be found in the Microsoft case[86]. Even if we have the technology that can solve this problem, finding an international middle term between the many legislators in the whole world about the way to transfer data in a safe and respectable way seems utopian.

In my opinion, the GDPR will not lead in, and to massive changes in the field of international data transfers for the EU to give the next relevant step. Considering that, we require other fields we need to focus on the role of additional technical protection measures, focusing on cybersecurity tools, that can help organisations using SCCs, main tool for data transfers, to provide the European level of protection when the data is flowing the world and possibly subject to public surveillance[87]. These measures include: the use of robust end-to-end encryption with one or more independent EU/EEA-based trustees securely holding the keys, and multi-party homomorphic encryption,[88] that

85 Kuner, Christopher, 2020.

86 United States District Court for The District of Columbia, United States of America V. Microsoft Corporation (5 November 1999). Available at: <https://www.justice.go v/sites/default/fil es/atr/legacy/2006/04/11/msjudge.pdf>

87 Compagnucci, Marcelo and Aboy, Mateo and Minssen, Timo, "Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)", page 11 and 12, 2021. Available at SSRN: <https://ssrn.com/abstract=3951085>

88 Marcelo Corrales Compagnucci and others, 'Homomorphic Encryption: The 'Holy Grail' for Big Data Analytics & Legal Compliance in the Pharmaceutical and Healthcare Sector?', European Pharmaceutical Law Review 3(4):144-155. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3488291>

should be implemented within an overall ISMS[89] and PIMS[90] that is properly scoped and regulatory stress-tested, but also independently audited through third-party certification audits (ISO27001/27701).

In short, the Court of Justice of the European Union is serious about the fundamental rights dimension of data protection, but also finding a balanced way to maintain the foundations of Safe Harbour and the transatlantic data transfer, probably with an evolved international law, tons of established treaties, but we can assure that we are getting a lot of case law in the coming years and new challenges with technological and security advancements in the Digital Era.

4. Elgizouli V Secretary of State for The Home Department: a gap in the international data transfer framework?

4.1. Context

Exactly at 11 p.m. GMT, on January 31st, 2020, the UK ceased to be a Member State of the EU. In terms of its impact on the adoption of the EU legal framework, it left the UK with the Data Protection Act 2018 (DPA), adding to the GDPR where Member States were allowed to regulate, and combined it with regulation for processing activities outside the scope of the GDPR, being created to be in force at the time that the exit was finalised.[91] Post-Brexit European legislation was no longer in force. However, the regimes will be shown to be near-identical, with the UK mirroring the European approach to data protection, namely in international data transfer.

4.2. The Case

Shafee El Sheikh, a former British citizen, was accused, in the USA, of being involved in terrorist activities and the murders of several US and British citizens. This happened due to links Mr El Sheikh shared with a terrorist

89 Information Security Management System (ISO 27001).

90 Privacy Information Management System (ISO 27701).

91 Celeste, Edoardo, Cross-Border Data Protection After Brexit, Brexit Institute, Brexit Institute Working Paper Series, No 4/2021, 2021, p.5. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784811>

organization based in Syria, acting in the context of the civil war.[92] The crimes listed bore special gruesomeness.[93]

On June 22nd, 2018, the SSHD[94] of the UK Government at the time, decided to grant a request made by the Government of the USA, under the MLA,[95] pursuant to this case. The request materially involved the sharing of personal data of the individuals identified by the US Government. Due to the grave nature of the crimes, and the permissibility of employing capital punishment as a penalty for crimes of this legal type within the US legal framework,[96] the SSHD sought guarantees about the avoidance of the death penalty in this particular case. The US DoJ[97] only assured that they would "introduce no evidence obtained in response to this request in a proceeding against any person for an offence subject to the death penalty. In the event that the evidence was to be introduced, the United States would take the decision not to seek the death penalty, a decision which in the federal system absolutely precludes the death penalty from being imposed.",[98] known as a "Direct Use" undertaking. This would not prevent the influence of the evidence provided by the SSHD in informing the investigation and could make it practically part of the chain of conduct that would lead to an eventual death penalty sentence. The information was later shown to US investigators merely on an "information-sharing basis" in February 2018.[99]

In January 2018 Mr El Sheikh was taken into custody, providing the beginning of legal and eventual court proceedings. The conversations between the US Attorney General, the SSHD and Security Minister for the UK began.

92 Why has the Syrian war lasted 10 years?, BBC News, 2021. Available at: <https://www.bbc.com/news/world-middle-east-35806229>

93 [EWHC 60 (Admin) Case No: CO/3449/2018, The Queen (on the application of Maha El Gizouli) And The Secretary Of State For The Home Department, 2019, The History, 5. and 6. Available at: <https://www.bailii.org/ew/cases/EWHC/Admin/2019/60.html>

94 Secretary of State for the Home Department.

95 1994 Treaty of Mutual Legal Assistance in Criminal Matters between the US and the UK.

96 "PATRIOT ACT II" PROVISIONS IN H.R. 10 (AS PASSED BY HOUSE), ACLU. Available at: <https://www.aclu.org/other/patriot-act-ii-provisions-hr-10-passed-house>

97 United States Department of Justice.

98 EWHC 60 (Admin) Case No: CO/3449/2018, The Queen (on the application of Maha El Gizouli) And The Secretary Of State For The Home Department, 2019, 8. Available at: <https://www.bailii.org/ew/cases/EWHC/Admin/2019/60.html>

99 Ibid. 12.

The UK decided not to try Mr El Sheikh, due to lack of evidence and sought to support the US in their attempt. Eventually, the cabinet of SSHD was succeeded and its new holder had a more favourable outlook on whether the death penalty should act as a deterrent to the acceptance of the request. Adding to this, the UK Ambassador in the US recognized the tension and that the need for assurance to not seek the death penalty might deter the US from prosecuting Mr El Sheikh and perhaps lead to his confinement to the Guantánamo Bay Detention Camp.[100] The SSHD maintained their fear of the strong contemporaneous political tensions regarding this matter and their concerns as to Mr El Sheikh's confinement to Guantánamo being a result. This culminated in the granting of the request by the SSHD in a letter to the US Attorney General in a letter, with a mention as to how "there are strong reasons for not requiring a death penalty assurance in this specific case, so no such assurances will be sought".[101]

Mr El Sheikh's mother, Ms El Gizouli, was the claimant in this case. She submitted her request, speaking on the effect the decision had on her, and also challenging its merits. She sought to declare the decision made was unlawful, set a precedent preventing the absence of said assurance, an order that forced the SSHD to secure the destruction or return of the data and demand and an assurance as to Guantánamo Bay.

A) The Ground

The initial complaint was submitted on several grounds, among which are: the illegality and breach of the rule of law, that the exception to the policy is inconsistent with its rationale, errors of law disclosed in the decision letter, the violation of the claimant's Convention rights and the unlawful transfer of personal data in breach of domestic and EU data protection law. For this work, it is of particular relevance to analyse the unlawful transfer of personal data in breach of domestic and EU data protection law. The data transfer in question took place a month after most of the DPA came into force. Seen as

100 Guantánamo Bay Detention Camp, ACLU. Available at: <https://www.aclu.org/issues/national-security/detention/guantanamo-bay-detention-camp>

101 EWHC 60 (Admin) Case No: CO/3449/2018, The Queen (on the application of Maha El Gizouli) And The Secretary Of State For The Home Department, 2019, 8. Available at: <https://www.bailii.org/ew/cases/EWHC/Admin/2019/60.html>

that this is a criminal investigation, aiming to originate criminal charges, and this information in question relates to that, it is inevitable that it qualifies as personal data, per the definition of both the DPA[102] and the GDPR.[103] It also doesn't qualify as personal data regulated under the GDPR scope as per the DPA[104] and GDPR[105] definitions, being that the data is being processed for criminal procedure purposes. It is abridged by Section 3 of the DPA, which is dedicated to the processing of personal data by the authorities competent to investigate criminal matters, as well as Directive 2016/680 of the EU,[106] also known as the Police Directive[107]. Their definitions of personal data still apply in spite of the different matter, maintaining the harmony that was aimed at during the big legislative efforts around the protection of said personal data.[108]

As article 29 of the DPA indicates, the following articles apply to the processing of the personal data category we previously mentioned by a competent authority, as defined by article 30 (1) (a) and Schedule 7, as well as a controller, as defined in article 32. In that way, the SSHD is subjected to this legislation and therefore, the legal demands for international data transfer considerations. The claim alleges that this is matter is international data transfer abridged by the law stated above and is in breach of sections 35 (lawful and fair data transfer demands) and 36 (the collection of data must be specified,

102 Data Protection Act 2018, Article 2 (1).

103 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), Article 4(1).

104 Data Protection Act 2018, Article 29.

105 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), Recital (19) and Article 2 (2) (d).

106 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

107 European Data Protection Supervisor, Police Directive. Available at: <https://edps.europa.eu/data-protection/our-work/subjects/police-directive_en>

108 Edgar, Michael, *Harmonising European data protection law Agreement reached on the General Data Protection Regulation*, Laytons Solicitors. Available at: <https://static1.squarespace.com/static/570665c1 d51cd45f7c8f1812/t/5824c62cf7e0ab32fa764efc/1478805039099/Harmonising+European+data+protection+law+Focus+Jan+2016.pdf>

explicit and legitimate, and the manner of collection can't be incompatible with the purpose of the collection), as well as the specific sections 73 to 76, the specific data transfer section, defining its general principles. These are complex principles, demanding 3 conditions be met in order to be fulfilled subsidiarily in the following order: adequacy, appropriate safeguards and special circumstances. There is a correlation with the Police Directive, with article 4 (1)(c), requiring adequacy, which is materialised in recital, and article 35 (1)(d) that establishes this subsidiarity in the same order with the same concepts in mind. The articles in both the legal diplomas are almost mirrored, although slightly more concretely stated in the Police Directive. Article 36, referred to the adequacy decision, the consideration taken into account can be summed up to abidance with the law on the plain of human rights, public security, defense, national security and criminal law, the existence of a proper supervisory authority, and the obligations the other party to the transfer has entered into. Articles 37 and 38, relating to the appropriate safeguards are practically identical to their equivalents in content and language. There are also special restrictions for the processing of the data in section 80 of the DPA regarding the application of the international data transfer section, ensuring that when faced with international data transfer, the restrictions applied for national data transfer are also transposed and enforced.

As we have seen before, there was no consideration of these matters of the law in the initial decision, which focused on the penal side.

B) The decision

The Court[109] decided against the claimant in this matter.

The data protection part of the claim begins by annulling the argument of the unfairness of the decision by way of interpretation of the concept as meaning material transparency with the data subject about the use of their data, moving on to the lawfulness criteria, that is set aside due to the court's understanding that the record-keeping needs not to be a "bespoke set of documents",[110] rendering the claimant's argument as lacking merit, and finally

109 England and Wales High Court (Administrative Court)

110 WHC 60 (Admin) Case No: CO/3449/2018, The Queen (on the application of Maha

that the argument for special circumstances, due to the claimant's classification of this matter as "sensitive processing", revealing to be a difficult matter for the court to assess due to not having actual possession of the information to be able to discern whether it contains "racial or ethnic origin, political opinions, religious or philosophical beliefs",[111] resulting in a rejection of claims regarding the First Data Protection Principle of the DPA.

The Second Data Protection Principle claims were equally dismissed in the context of the court considering the intent to aid in a foreign prosecution was probably there from the start of the investigation, when the evidence was being collected, and that the means were proportionate.

The part of the claim regarding the transfer of personal data to a third country follows the same path of dismissal through the court considering every condition to be met and that the requirements are not necessarily expressly regarded, rather than the substantive reality secures the appropriate safeguards, excusing the SSHD as a consequence of considering they duly evaluated all possibilities, and the solution was necessary.

Lastly, with regards to the special processing restrictions, the claim was dismissed by way of considering that the section at hand cannot be subjected to the use as a way to manipulate a third country's sentencing law and shouldn't be a deterrent from applying to the MLA.

The appeal resulted in a similar outcome.[112]

4.3. European Law considerations

As we have been able to gather, Brexit impacted the application of European law in the UK. The final Brexit agreement provided that the UK would become one of the non-member-state countries with the closest framework in the area of data protection to the EU framework. Due to their

---

El Gizouli) And The Secretary Of State For The Home Department, 2019, 189. Available at: <https://www.bailii.org/ew/cases/EWHC/Admin/2019/60.html>

111 Ibid. 191.

112 EWHC 2516 (Admin) Case No: CO/3082/2020, The Queen (On Application Of Maha Elgizouli) And The Secretary Of State For The Home Department And Director Of Public Prosecutions, 2020, 65. Available at: <https://www.judiciary.uk/ wp-content/uploads/2020/09/ Elgizouli-v-SoS-Judgment.pdf>

five-decade long presence in the EU and the consequent adoption of all its directives, the aforementioned DPA, the national transposition of the Data Protection Directives[113] and the UK GDPR all reflect the European legal vision.

The Police Directive shows itself as the EU's attempt to bring forth international cooperation on data protection and international criminal prosecution.[114] It also shows itself as not an attempt to interfere with other countries' legal frameworks, imposing the European boundaries onto other countries which have different views on the definition of criminal types.[115] There is still the question regarding the possibility of the death penalty, the one that arose. There is a lot of legal discourse around whether the death penalty is a violation of human rights.[116] Article 2 of the EUCFR states in its article 2(2) that no person may be sentenced to the death penalty or executed. This is legislation that applies to European space. However, it is essentially a list of the values the union upholds above all and the question arises: even if in regards to a third country that supports this that would be considered a cruel and unusual punishment in the European space, should we override the principles of international cooperation, non-interference with external law application, and the basic layout defined by the data protection framework, when contributing to possible employment of the death penalty?

The truth is that this is a complicated matter. Lord Kerr, the dissenting justice in the appeal, marked a strong opinion against allowing the contribution of the UK to a possible death penalty, enhancing how the common law has not yet evolved in this matter, even though it is custom that the UK Government

113 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

114 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Recital (7).

115 Ibid. Recital (14)

116 Charter of Fundamental Rights of the European Union. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=PT>

rejects any employment of the death penalty, and the UK, as well as European countries, do not perform extraditions, deportations and other transfers of people without assurance.[117] It would seem coherent and also withhold evidence without assurances, given the extreme importance of safeguarding lives. Besides that, as Lord Kerr points out, the law is ever evolving and meant to reflect the morals and values of the contemporaneous society. With an ever-growing number of countries joining the abolitionist group, more than doubling between 1991 and 2017,[118] reflecting the undeniable majority of countries in the world, it is not only logical according to the framing of the legal provisions, but also reflective of the ideals shared among the world that life should trump any other interest at stake.

4.4. Should the "Police Directive" be adapted?

Data protection has become a very demanding and pressing question in the digital age. The rise in technology provided the ability to store, process and use unprecedented amounts of data for any purpose imaginable. This has also begun taking a toll on individuals. That is the context for the emergence of regulations such as the Police Directive. Would it make sense, given the circumstances of this case and the very real possibilities that it may reoccur, to alter the data protection directive that resolves this matter?

In its recitals, the Directive informs on how its conception can be associated with the increased technological advancements and the insecurities that follow them.[119] Criminal Authorities can now store that more data and the process becomes increasingly less transparent to the data subject, that does not necessarily have the capabilities to screen. This Directive was created for

117 Human Rights Committee, General comment No. 36 (2018) on article 6 of the International Covenant on Civil and Political Rights, on the right to life, 30. Available at: <https:// tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/1_Global/CCPR_C_GC_36_8785_E.pdf>

118 *Death penalty: How many countries still have it?*, BBC News, 2020. Available at: <https://www.bbc.co m/news/world-45835584>

119 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Recital (3)

that reason, to ensure that every individual is duly protected from the parties holding the power: in this case, the competent authorities. Whether it be a data protection authority, the criminal authority, or any branch of the government, these institutions may not be the most transparent when not needed, in order to facilitate the accomplishment of their goals. Ensuring that all the international data transfer is subjected to a final threshold of passing the non-facilitating test,[120] perhaps inside the sequence established in article 35, safeguarding that in any case that capital punishment is at play, the obligation to obtain assurance. Or perhaps the next occurrence of a similar case will be within the EU Member-States and may be appealed all the way up to becoming European case law with some force and incentivize the law to be interpreted in that way.

4.5. Data Governance as a means of intimidation?

The final question regards the potential to use this gap in the law that allows European nations to tacitly condone the death penalty by way of inaction is the lack of legal certainty. It is in fact customary for these types of international data exchanges to come accompanied with assurances, as the UK has this as the bastion of case law on the matter. However, with a precedent of admissibility of interpretation, and in spite of Brexit, we now have a clear avenue that governments can use to take advantage of the delay of other countries in matters of death penalty abolition for political gains.

This particular matter was decided due to heavy political tension and many moments of attempted negotiation, but the result was the lack of protection of a person's right to life that the UK was in a position to assure. Can wars begin to be waged by these means? Can countries effectively begin to use international cases and hold data hostage to bargain for political envisionments of the result? A reality in which the sharing of personal data is decided through political manoeuvring may result in countries outside the EU leveraging commercial benefits, economic partnerships and other political liaisons to pressure European Governments into conceding on matters of this regard. The

120 Based on the *"non-facilitation argument"*, Hilary Term [2020] UKSC 10 On appeal from: [2019] EWHC 60 (Admin), 68. Available at: <https://www.supremecourt.uk/cases/docs/uksc-2019-0057 -judgment.pdf>

SSHD was not entirely resistant to the idea at the moment of taking office. They were nevertheless bent to the will of the US Attorney and Government, who were threatening to possibly subject Mr El Sheikh to an almost certainly worse fate being held in Guantánamo. The SSHD bent to that will due to not having enough bargaining chips at the moment and having the decisions in their hands. The solution pointed to above to make a written declaration of legal obligation in the Police Directive would end the ability to negotiate and set the bargain in stone for states outside the EU that do allow for this type of punishment.

5. The Recent Case of the Russian Protesters and Portugal's Breach of the GDPR

5.1. Factual context

The GDPR is strongly committed to the protection of the rights recognized to individuals, not only concerning their data, but also the circumscribed fundamental rights, and although it applies mandatorily only in the countries of the European Union, it is not disconnected from the reality in which we live.

Today's globalized and digital society, which allows (and even "forces") us to be increasingly connected and seems to facilitate everyday processes, often reveals "the other side of the coin", bringing new challenges and problems and, with them, new dangers for individuals, who are increasingly exposed to possible violations of their rights, recognized and enshrined in various international texts.

That said, in this chapter will be analyzed a recent case, occurred in Portugal, where these issues will be addressed, in a critical way, and having the final goal of sketching directions for the future of the Union regarding specifically the issue of data transfers to third countries and the underlying relationship with fundamental rights.

The case began in January 2021 when the Lisbon Municipality breached the GDPR by illegally transferring the names, addresses, and contact details of three individuals who took part in a protest in Lisbon for the release of Alexey

Navalny, an opponent of Vladimir Putin's regime,[121]to the Russian Embassy, without any legal justification.

The Municipality did not seek to legitimize its actions, admitting that the transfer of the data in question was "inadequate".[122] As a "justification", it only pointed out the "lack of updating of bureaucratic procedures" related to the organization of demonstrations. According to CML, what happened was that, in compliance with Decree-Law 406/74 of 29 August, which regulates the right of assembly in Portugal, "«(...) the data of the three organizers was received" and that this information was "sent by CML's technical services to PSP/MAI and the entity/location of the demonstration (in this case, the Russian embassy of consular services), under the general procedure adopted for demonstrations »."."[123]

Thus, instead of informing only of the event, since it would take place in front of the Embassy, it advanced the personal data of the demonstrators, "(...) when the law does not expressly provide for the sending of this specific data".[124]

The National Commission for Data Protection (the Portuguese supervisory authority) has already opened an enquiry to ascertain the facts and the applicable consequences. However, since we do not have much information so far, this section will focus on a strictly academic analysis of what may be the implications in question.

5.2. Transfer of personal data to a third country

The extent of the concept of "data transfer" has been much debated in European doctrine and jurisprudence, as the GDPR has chosen not to expressly

121 Agência Lusa, *Comissão de Proteção de Dados abre inquérito a partilha de dados com a Rússia*, Observador, 2021. Available at: <https://observador.pt/2021/06/10/comissao-de-protecao-de-dad os-abre-inquerito-a-partilha-de-dados-com-a-russia/>

122 Ibid.

123 Lusa, *Câmara de Lisboa alterou os procedimentos de partilha de dados de manifestantes após caso Navalny*, Sapo, 2021. Available at: <https://www.sapo.pt/noticias/atualidade/camara-de-lisboa -alterou-procedimentos-de_60c1e615dba1497270e1df38>

124 Joana Petiz, *"Nada justifica a quebra da Proteção de Dados" e pode haver "responsabilidade criminal"*, Dinheiro Vivo, 2021. Available at: <https://www.dinheirovivo.pt/economia/nada-justifica-a-quebra-da-protecao-de-dados-e-pode-haver-responsabilidade-criminal-13828603.html>

adopt a definition.

When questioned, the European Commission departed from existing positions,[125] clarifying that "the term is often associated with an act of sending or transmitting personal data from one country to another, for example by sending paper or electronic documents containing personal data by post or email. Other situations that also fit this definition are all cases where there is an action of the controller to make personal data available to a third party located in a third country".[126]

This concept has also been discussed in case law, particularly in the *Lindqvist, Schrems* and *Schrems II* cases. However, with the indications of the Commission and the case law, we may conclude that in the present case we are dealing with a transfer of data, insofar it was an act of transmission of personal data, in electronic format, to a third country.

Concerning the definition of "third country", and although the Regulation once again does not specifically define what is to be understood by this concept, by recourse to Article 3 *a contrario sensu* GDPR we can extract that a third country is one that is not "situated in the territory of the Union". The European Commission has also clarified that a third country is a "country that is not a member of the EU".[127]

It is to be noted that the Embassies are a case of "extension of the application of national data protection legislation beyond national borders",[128] which means the Embassy is subject to Russian legislation, not the GDPR, even if located in Portugal.

Since Russia is not an EU Member State, it is considered a third country for the purposes of applying this Regulation, which requires an analysis of Chapter V, but also of the general rules and principles provided, first of all, in

125 Namely, the G29's position.

126 European Commission, "Frequently Asked Questions Relating To Transfers of Personal Data From the EU/EEA to Third Countries", 2009, cit., p. 18 via Moniz, Maria da Graça, 2018, pp. 242-243.

127 European Commission, "What rules apply if my organization transfers data outside the EU?". Available at: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pt>

128 G29, "Parecer 8/2010 sobre a lei aplicável", 16 de dezembro de 2010, cit., p. 30 via Moniz, Maria da Graça, 2018, p. 137.

Article 5, because although these data transfers are possible, it is necessary having in mind that "(the) protection granted by the Regulation (...) travels with the data, which means that the rules protecting personal data continue to apply regardless of where the data is located".[129]

As such, for data to be transferred from the EU, with the assurance that it will continue to have the same level of protection in a third country, certain conditions need to be met, as we will see below.

5.3. The absence of legal justification for the transfer of data

The GDPR dedicates its Chapter V and recitals 101 to 116 to the transfer of data to third countries, making it clear in article 44 GDPR that despite the intention to maintain the international relations in the field of personal data, this will only be possible if "(...) the conditions set out in this Chapter are respected by the controller (...)" and "(...) the level of protection of natural persons guaranteed by this Regulation is not undermined". To ensure such protection, the following articles underline conditions that must be met.

Firstly, Article 45(1) provides that "a transfer of personal data to a third country may take place where the Commission has decided that the country (...) ensures an adequate level of protection". After assessment of the level of protection, according to the criteria defined in the following paragraphs of the article in question, paragraph 8 dictates that "the Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries (...) which it has decided that an adequate level of protection is (...) ensured" and to which the Member States may transfer personal data.

From an analysis of the *Journal's website*, it appears that the Commission does not consider that Russia guarantees an adequate level of protection,[130] which means an EU Member State may not transfer data to that territory based on an "adequacy decision". In the present case, Portugal could not have sent the data on this basis.

---

129 Ibid.

130 European Commission, "Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection.". Available at: <https://ec.europa.eu/info/law/law-top ic/data-protection/international-dimension-data-protection/adequacy-decisions_pt>

Even if there is no such decision, article 46 GDPR presents another way to legitimise the sending of personal data to third countries, through its subjection to "appropriate safeguards" offered by the third country, and on the assumption that the data subjects enjoy "enforceable rights" and "effective legal remedies". The article also sets various means of providing these safeguards.

However, none of these predictions apply in this case, as CML sent the data without even being requested by Russia, which means this country did not present *a priori* any kind of adequate guarantees to justify the transfer.

Finally, article 49 cannot be resorted to either, since the situation in question does not fit the provision of any of its subparagraphs, not even in (d), which seeks to ground a transfer on "important reasons of public interest". A demonstration that has met the legal requirements and in the terms already described cannot, under any circumstances, fall within this criterion.

Furthermore, since that was a demonstration in favour of the release of an individual who has been imprisoned for opposing the regime of Vladimir Putin, even if the data sent appears to be content-neutral, it seems that we are, in reality, facing data revealing political opinions, considered a special category of data in Article 9 GDPR, whose processing is generally prohibited, and which makes the error committed by Portugal further compounded.

Although paragraph 2 presents exceptions to this prohibition, the concrete case does not seem to fit in any of the subparagraphs: it was not a legal obligation (paragraph b)), since the Portuguese decree on demonstrations does not impose the sharing of personal data of demonstrators; nor a transfer on public interest ground, since none of the requirements imposed by the subparagraph are met (*i.e.* the need for processing for reasons of public interest, the proportionality requirement, the respect for the essence of the right to the protection of personal data and the protection of the fundamental rights and interests of data subjects).

Finally, and as mentioned, although Chapter V enshrines the legal provisions regarding data transfers, the general principles and rules of the Regulation must be respected. Among these, we find lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability (article 5).

However, having arrived here, we have already concluded that CML, responsible for the data processing, has ignored both specific provisions of Chapter V and the general principles and rules of GDPR.

5.4. The fundamental rights at stake and remedies for right holders

As mentioned at the beginning of this chapter, the GDPR plays a pivotal role in protecting the rights of data subjects. Although instruments such as the Charter of Fundamental Rights of the European Union and the TFEU already ensure this same role, enshrining the right to the protection of personal data in their articles 8 and 16, respectively, the GDPR goes further. First of all, because it allows us to better understand the essence of this right in its recital 7, when it states that "natural persons should have control of their own personal", linking it to a "dynamic right" - the right to informational self-determination (*i.e.*, the right to control one's data).

However, it is necessary to be aware that there are other "concerns about the risks to fundamental rights arising from new processing of personal data triggered by technological development"[131] which go beyond the right to data protection in its strictest sense. It is now undeniable that "the processing of personal data poses risks to other fundamental rights",[132] which is immediately recognized by the GDPR, in its first article, and which lead authors to argue that this fundamental right, although autonomous from all the others, plays a role of "guarantee right"[133] by cherishing the protection of other fundamental rights, with which it has a "direct link".[134]

That said, it is now clear that the violation committed by the CML is even more serious than it might seem, as it is not just personal data as "simple data" that are at stake, but also what the disregard for this right means for the "dignity of the human person, freedom (of action, expression, thought),

131 Moniz, Maria da Graça, 2018, p. 67.

132 Mañas, José Piñar, "Objeto del reglamento", J. Piñar Mañas, *Reglamento General,* cit., p. 56 e ss. via MONIZ, Maria da Graça, 2018, p. 72.

133 Moniz, Maria da Graça, 2018, p. 72.

134 Calvão, Filipa, "Direito da Proteção de Dados Pessoais", Universidade Católica, Lisboa, 2018, cit., p. 51 via Moniz, Maria da Graça, 2018, p. 72.

autonomy, self-determination, personal identity, social participation"[135] and privacy of the three protesters.

Regarding remedies, data subjects in these circumstances are entitled to complain to a supervisory authority, by application of article 77 GDPR. In Portugal, the supervisory authority is the CNPD, as stated in article 3 of the Law No. 58/2019. In the present case, this complaint has been properly carried out.

In addition to this right, they can also take legal action against the controller, as provided in article 79. Once again, in the case under analysis, the protesters stated their intention to take the case to court against CML, mainly to prevent situations like this from happening again.

5.5. Accountability and other legal consequences

As regards the legal consequences for the Municipality, article 82 determines that if the existence of damages resulting from such breach is proven, it will be held liable and the three demonstrators will be entitled to compensation.

Furthermore, the Regulation provides for the imposition of fines due to its violation in article 83, which should be applied in the case under analysis. The amount will have to be determined by the NCDP according to the criteria set in paragraph 2. Paragraph 5 (c) further clarifies that the violation of the provisions on transfers of personal data according to articles 44 to 49 is subject to a fine of up to EUR 20 000 000. In this sense goes also Law No. 58/2019, in its articles 37 and 39.

Also, it is worth mentioning article 84 GDPR, which delegates to the Member States the establishment of other sanctions in addition to those already provided for in the Regulation.

---

135 Rouvroy, Antoinette e Poullet, Yves "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", Serge Gutwirth et *alii* (eds.), *Reinventing Data Protection?,* Springer, 2009, cit., p. 47 e ss.; Calvão, Filipa, "O direito fundamental à proteção dos dados pessoais e a privacidade 40 anos depois", Manuel A. VAZ *et alii, Jornadas nos quarenta anos da constituição da república portuguesa*, Universidade Católica, 2017, cit., p. 88 via Moniz, Maria da Graça, 2018, p. 72.

Therefore, article 46 of Law no. 58/2019 determines in paragraph 1 that "Whoever uses personal data in a manner incompatible with the determining purpose of the collection shall be punished by imprisonment of up to one year or a fine of up to 120 days". However, since we are dealing with the special data category of article 9, the penalty is doubled in its limits, as established in paragraph 2.

This diploma also determines in article 48 (1) that "whoever (...) transfers, for payment or free of charge, personal data without legal provision or consent, regardless of the purpose pursued, shall be punished with imprisonment of up to 1 year or with a fine of up to 120 days". Once again, the penalty is doubled in its limits since personal data referred to in article 9 is involved (paragraph 2). The identification of the concrete persons within CML responsible for the violation of the GDPR, who may suffer these penalties, will be verified during the enquiry already opened by the National Commission for Data Protection.

5.6. Final critique

The law is of little use if it only exists on paper. It needs to be respected. Although it enshrines ways to correct damage, the purpose of the law is to prevent such damage from happening, serving as a "guide" to action. And this goes for any law, whether it applies to individuals or legal entities, private or public sector.

However, since public entities are the authorities that run our country, it is unacceptable that they do not comply with the law, violating citizens' rights and even putting their lives at risk. It would be expected for their behaviour to serve as an example to their citizens, but unfortunately this is not the case.

As analyzed, Russia is not considered by the Commission to provide an adequate level of protection, nor is it a country known for respecting human rights (other than on paper). It indeed is one of the signatory countries to several international texts, in particular the Universal Declaration of Human Rights, but that does not mean the protection of rights exists in practice and not just on the formal level. This means that Portugal not only acted illegally, but also put the lives of three persons at risk.

In all these behaviours from State authorities, there is a common factor: the abuse of power concerning its citizens. It is vital to find ways to make sure that public authorities respect the law and not just subsequently accept the consequences that come from the abuses committed, since in such cases the damage to citizens will always be more severe than the consequences applied.

That said, and with the goal to maintain a climate of harmony between states and between public authorities and citizens, with respect for their fundamental rights, the EU shall always demand from Member States an outstanding behaviour *a priori* and, failing that, determine heavy consequences with a preventive function, in order to stop the abuses and actually protect individuals.

6. Conclusion

This work gives a broad overview of the many issues concerning the regulation of transborder data flows and raises some relevant questions in regards to future data protection possible alterations. Jurisdictions with different data privacy rules could cooperate to manage and facilitate the flows of data between them, and ensure national security and defense; corporations have an important role in international data transfers and cyberterrorism must be a matter of preoccupation.

Countries show a diversity of approaches to "trans-data" regulation, having as the main tension point the polarity of legal orders, like the EU's, that use the determination of *adequacy* of data protection in foreign jurisdictions as criteria, such as shown regarding the United States, and those that are more organizationally-based, using the *accountability* principle. This tension does not only regard data protection and privacy regulation, but of any regulation that is territorially-based, like most data protection and privacy law[136]. It is important to state that while regulation of capital flows and international trade has been liberalized in the last few decades, the regulation of transborder data

136 Kuner, Christopher, *Regulation of Transborder Data Flows Under Data Protection and Privacy L*aw: Past, Present, and Future (October 1, 2010). TILT Law & Technology Working Paper No. 016/2010, Tilburg Law School Research Paper No. 016/2010, page 39. Available at SSRN: <https://ssrn.com/abst ract=1689483≥

flows has been tightened, due, also, to the European acknowledgment that the data subjects are exposed to permissiveness of some countries so that their data processed for more purposes than should be required. Even with that it's not enough to find a common international port.

The only conclusion possible is that international data transfers give way to political tensions that are enhanced by the differences in criteria, especially with the crescent importance and popular attention paid to personal data related matters. It is imperative that these may be put aside, and a mostly harmonized legal order is incentivized to reduce conflict, block out political strategy, and focus on the protection of the party who this regime was created to protect: the natural person.

Direito de Oposição à Definição de Perfis

SÉRGIO MIGUEL JOSÉ CORREIA[*]

Resumo: Contrariamente ao que ocorria com a Diretiva 95/46/CE, o Regulamento Geral sobre a Proteção de Dados aborda a temática da definição de perfis com especial atenção. Atendendo aos riscos inerentes a este tipo de tratamento de dados pessoais, são colocados à disposição do titular dos dados vários meios de defesa, entre os quais se situa o direito de oposição. No presente estudo, explora-se aquilo em que consiste a definição de perfis, os perigos e malefícios a si associados e os contornos do acionamento daquele poder de reação atribuído ao titular dos dados.

***Palavras-chave**: Definição de perfis; direito de oposição; tratamento de dados pessoais; comercialização direta; Regulamento Geral sobre a Proteção de Dados.*

Abstract: Contrary to the Directive 95/46/EC, the General Data Protection Regulation addresses the issue of profiling with special attention. Given the inherent risks of this type of processing of personal data, various means of defense are made available to the data subject, amongst them being the right to object. This study explores what is profiling, the dangers and harms associated with it and the contours of the aforementioned right attributed to the data subject.

***Keywords**: Profiling; right to object; processing of personal data; direct marketing; General Data Protection Regulation.*

[*] Licenciado e Mestre em Direito e Prática Jurídica, Especialidade de Direito Civil, pela Faculdade de Direito da Universidade de Lisboa. Pós-Graduado em Direito da Proteção de Dados, pelo Centro de Investigação de Direito Privado da Faculdade de Direito da Universidade de Lisboa.

1. Considerações Iniciais

A globalização e a forte e rápida evolução tecnológica têm contribuído para um crescimento enfático na quantidade de dados pessoais constantemente obtidos quer pelas empresas privadas, quer pelas entidades públicas. Não é de todo exagerado afirmar que o volume de informações pessoais hoje armazenado pelos diversos responsáveis pelo tratamento é vastamente superior àquele que nós detemos sobre as nossas próprias vidas[1].

Para além disto, ininterruptamente constatam-se impulsos e avanços no domínio da Inteligência Artificial (*Artificial Intelligence – AI*) e da aprendizagem automática (*machine learning*), da *Big Data* e da Internet de Coisas (*Internet of Things – IoT*), que têm ocasionado um aumento da capacidade dos sistemas automatizados para encontrarem correlações e gerarem ligações entre os dados processados, o que permite determinar, analisar e antever aspetos próprios das pessoas, relacionados, entre outros, com as suas personalidades, comportamentos, interesses e hábitos[2].

Nesta conjuntura, a definição de perfis tem encontrado amplo espaço para se desenvolver e atravessar os mais diversos setores: as instituições de crédito recorrem a esta prática para efeitos de *credit scoring*[3]; as seguradoras utilizam a definição de perfis, mormente, com intuitos estatísticos e atuariais, de modo a avaliar e determinar o risco e o prémio para a conclusão e execução

1 Cordeiro, A. Barreto Menezes, *Direito da Proteção de Dados – À Luz do RGPD e da Lei N.º 58/2019*, Almedina, 2020, p. 29.

2 WP 29, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, WP251rev.01, Adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, p. 5, disponível em <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>, consultado a 22 de dezembro de 2021.

3 "A análise do risco de crédito do cliente corresponde a uma fase determinante no processo de tomada de decisão do banco relativamente à concessão de crédito a um cliente. Dessa análise […] resultará a atribuição de um grau de risco (*risk rating*) e de uma classificação ao cliente (*scoring*), aos quais se associa o nível de *merecimento de crédito* deste. Os fatores considerados nesta avaliação prendem-se com características e circunstâncias associadas ao cliente. Será em função destes resultados que o banco vai decidir a elegibilidade do cliente para a concessão de crédito" – cf. Leal, Ana Alves, "Aspetos Jurídicos da Análise de Dados na Internet (*Big Data Analytics*) Nos Setores Bancário e Financeiro: Proteção de Dados Pessoais e Deveres de Informação" *in* Cordeiro, António Menezes, Oliveira, Ana Perestrelo de. Duarte, Diogo Pereira (Coord.), *FinTech – Desafios da Tecnologia Financeira*, Almedina, 2017, pp. 75-202, p. 197.

dos contratos de seguro; e na esfera do *marketing* esta técnica serve para melhor dirigir anúncios publicitários de bens e serviços a consumidores com determinadas características, qualidades e elementos pretendidos em comum, ou seja, ao público-alvo. É evidente que os casos expostos não esgotam o universo de atuação da definição de perfis, nem as finalidades para as quais se emprega o dito exercício, contudo não deixam de servir o objetivo de destacar a presença daquela forma de tratamento de dados pessoais na vida quotidiana.

O termo "perfil" refere-se a um conjunto de dados que caracteriza uma determinada categoria de pessoas, categoria esta que servirá para qualificar um certo sujeito[4]. Essencialmente, com a definição de perfis, procede-se à organização de pessoas em grupos de acordo com elementos, qualidades e características comuns, tendo em vista um certo propósito.

Não obstante tratar-se de um exercício com elevadas potencialidades nos mais diversos setores e atividades, comportando benefícios para as pessoas, a economia e a sociedade em geral, a definição de perfis não deixa de corresponder a uma atividade indissociável de sérios riscos e transtornos que não merecem ser desvirtuados. Com isto, justifica-se explorar aquilo em que consiste a definição de perfis, a sua perniciosidade, bem como um dos principais meios de defesa conferidos pelo Regulamento Geral sobre a Proteção de Dados[5] ao titular dos dados pessoais: o direito de oposição.

2. Definições de Perfis: Conceito e Elementos Caracterizadores

I. O Regulamento delineia que a definição de perfis (*profiling*) corresponde a "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados para avaliar certos aspetos pessoais de uma pessoa, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências

4 CoE, The Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling, Recommendation CM/Rec(2010)13 and Explanatory Memorandum, Council of Europe Publishing, 2011, pp. 9 e 38, para. 95, disponível em <https://rm.coe.int/16807096c3>, conultado a 22 de dezembro de 2021.

5 Regulamento (EU) 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 – de ora em diante, tão-só, RGPD ou Regulamento.

pessoais, interesses, fiabilidade, comportamento, localização ou deslocações" (art. 4.º, n.º 4, do RGPD).

O vocábulo "tratamento" representa "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (art. 4.º, n.º 2, do RGPD). A inclusão da expressão "tais como", na definição de tratamento, reflete a natureza não taxativa do elenco apresentado naquele mesmo preceito.

Assim, o *profiling* configura uma subcategoria de tratamento de dados pessoais[6] constituída por três elementos centrais: *(i)* tratamento automatizado; *(ii)* de dados pessoais; *(iii)* com o propósito de avaliar certos aspetos dos titulares[7].

II. O primeiro requisito demanda a existência de uma forma de tratamento automatizado. Decorre do n.º 1 do art. 2.º do RGPD que o Regulamento é aplicável ao tratamento de dados pessoais por *meios total ou parcialmente automatizados*, bem como ao tratamento por *meios não automatizados* de dados pessoais contidos em ficheiros ou a eles destinados. Configuram-se, assim, três níveis gradativos de automatização dos meios empregues no tratamento: não automatizados, parcialmente automatizados e totalmente automatizados.

O Regulamento não fornece uma conceção daquilo que são meios automatizados. Não o faz acertadamente! Dado os inevitáveis pulos tecnológicos, rapidamente a definição proposta de automatização tornar-se-ia obsoleta, além de que a sua consagração possibilitaria que fosse contornada a

6 Oliveira, Madalena Perestrelo de. "Definição de Perfis e Decisões Individuais Automatizadas no Regulamento Geral sobre a Proteção de Dados" *in* Cordeiro, António Menezes / Oliveira, Ana Perestrelo de / Duarte, Diogo Pereira (Coord.), *FinTech II – Novos Estudos sobre Tecnologia Financeira*, Almedina, 2019, pp. 61-88, p. 68.

7 WP 29, *Guidelines* cit., pp. 6-7; Oliveira, Madalena Perestrelo de. "Definição de Perfis" cit., p. 68; e Cordeiro, A. Barreto Menezes, *Direito* cit., p. 148.

proteção das pessoas[8] com fundamento, precisamente, no conteúdo positivado[9].

Sem embargo, entende-se que o tratamento por meios automatizados consiste em "operações sobre dados pessoais que envolvam equipamentos de processamento de dados, numa aceção ampla"[10]. Enquanto a aceção restrita da expressão corresponde a operações sobre dados pessoais que envolvem única e exclusivamente equipamentos de processamento de dados, a aceção ampla concede lugar à conjugação destes equipamentos com uma intervenção humana circunscrita, englobando, assim, o tratamento total e parcialmente automatizado. Por seu turno, a expressão tratamento por meios não automatizados refere-se a operações sobre dados pessoais que não incluam o recurso a quaisquer equipamentos de processamento de dados[11].

Com isto, os distintos graus de automatização, previamente apresentados, podem ser delimitados nos seguintes termos: *(i)* o tratamento de dados pessoais por meios totalmente automatizados não detém intervenção humana; *(ii)* o tratamento de dados pessoais por meios parcialmente automatizados embarca uma intervenção humana limitada; e *(iii)* o tratamento por meios não automatizados é uma expressão sinonima de tratamentos manuais[12].

Assim, quando o Regulamento indica que a definição de perfis corresponde a um tratamento automatizado (art. 4.º, n.º 4, 1ª parte, do RGPD), exclui do domínio do *profiling* os tratamentos por meios não automatizados, ou seja, os tratamentos manuais. Isto, porém, não significa o afastamento dos tratamentos parcialmente automatizados: a 1ª parte do n.º 4 do art. 4.º do RGPD menciona de modo expresso "qualquer forma de tratamento automatizado" e não "tratamento exclusivamente automatizado"[13]. A intervenção humana não adultera a essência do *profiling*, desde que restringida ou limitada, pois o que a definição de perfis exige é alguma forma (total ou parcial) de tratamento

8 Cf. Considerando 15 do RGPD, o qual acrescenta que a proteção das pessoas deverá, por aqueles motivos, ser neutra em termos tecnológicos e deverá ser independente das técnicas utilizadas. Trata-se do princípio da neutralidade tecnológica.

9 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 85.

10 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 85.

11 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 85.

12 Cordeiro, A. Barreto Menezes, *Direito* cit., pp. 85-86.

13 WP 29, *Guidelines* cit. p. 7.

automatizado[14/15].

III. O segundo elemento característico da definição de perfis é o de o tratamento automatizado ser efetuado sobre dados pessoais[16]. Consideram-se dados pessoais a informação relativa a uma pessoa singular identificada ou identificável (art. 4.º, n.º 1, 1ª parte, do RGPD). Sobressaltam, assim, quatro elementos particulares: *(i)* qualquer informação; *(ii)* relativa a; *(iii)* pessoa singular; e *(iv)* identificada ou identificável[17].

Primeiramente, toda a informação pessoal é considerada relevante: da perspetiva do *conteúdo*[18], toda a informação é merecedora de proteção jurídica, por muito fútil ou insignificante que possa aparentar[19]. Nesta ordem de ideias, o conceito de dados pessoais engloba todos os aspetos atinentes à pessoa (incluindo as suas crenças, desejos, posições políticas ou religiosas)[20], assumindo uma verdadeira flexibilidade e uma extensão ampla[21]. Quanto à *natureza*, o conceito de informação alberga tanto dados objetivos ou factuais, como dados subjetivos (designadamente, opiniões e avaliações subjetivas[22])[23].

---

14 WP 29, *Guidelines* cit., p. 7; Oliveira, Madalena Perestrelo de. "Definição de Perfis" cit., p. 68; e Cordeiro, A. Barreto Menezes, *Direito* cit., p. 149.

15 *Prima facie*, a avaliação dos aspetos pessoais do titular dos dados decorrerá por via de processos algorítmicos – cf. Cordeiro, A. Barreto Menezes, *Direito* cit., p. 149 –, uma vez que o *profiling* envolve estabelecer correlações entre vários conjuntos de informações de modo a efetuar inferências e deduções estatísticas e probabilísticas; tarefa que, de um prisma humano, revela-se extremamente difícil ou até impossível, atendendo à complexidade de todo o procedimento – cf. Oliveira, Madalena Perestrelo de, "Definição de Perfis" cit., p. 68; e CoE, *The Protection* cit., p. 39, para. 97.

16 Conquanto não se imponha a necessidade de efetuar uma análise exaustiva sobre a noção de dados pessoais, há que apresentar os seus pontos mais pertinentes.

17 WP 29, *Opinion 4/2007 on the Concept of Personal Data*, WP 136, Adotado em 20 de junho de 2007, p. 6, disponível em <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>, consultado a 22 de dezembro de 2021; e Cordeiro, A. Barreto Menezes, "Dados Pessoais: Conceito, Extensão e Limites", *Revista de Direito Civil*, III, 2, 2018, pp. 297-321, p. 300.

18 WP 29, *Opinion 4/2007* cit., p. 6.

19 Cordeiro, A. Barreto Menezes, "Dados Pessoais" cit., p. 301.

20 WP 29, *Opinion 4/2007* cit., pp. 6-7; e Cordeiro, A. Barreto Menezes, "Dados Pessoais" cit., p. 302.

21 WP 29, *Opinion 4/2007* cit., p. 6.

22 As opiniões e avaliações subjetivas são muito frequentes, por exemplo, na área laboral e no setor bancário e segurador. Assim sendo, são dados pessoais as seguintes informações: "*A* é um bom trabalhador e merece ser promovido"; "*B* não é uma pessoa confiável no que tange ao cumprimento das suas obrigações"; e "não é provável que *C* morra brevemente". Cf. WP 29, *Opinion 4/2007* cit., p. 6.

23 WP 29, *Opinion 4/2007* cit., p. 6; e Cordeiro, A. Barreto Menezes, "Dados Pessoais"

Por seu turno, enquadra-se dentro da noção de dados pessoais a informação disponível em qualquer *formato* (*v.g.*, alfabético, gráfico, numérico ou fotográfico) e constante de qualquer suporte[24].

Em segundo lugar, a informação tem de ser relativa a uma pessoa, isto é, tem de haver uma relação entre a informação e um sujeito[25]. Sem prejuízo disto, muitas vezes as informações relacionadas com objetos, podem, indiretamente, dizer respeito a pessoas[26/27/28]. Tipicamente, os objetos pertencem a alguém, as pessoas detêm algum tipo de influência sobre os objetos ou vice-versa, ou os objetos têm alguma proximidade com sujeitos ou demais objetos[29].

É possível apontar três situações em que se pode afirmar que os dados são relativos a uma pessoa. A primeira diz respeito ao *conteúdo*: a informação é relativa à pessoa se incidir sobre esta, ou seja, se for sobre ela[30]. A segunda situação reporta-se à *finalidade*: os dados serão relativos a alguém se forem utilizados com o propósito de avaliar, tratar de determinada forma ou influenciar o seu estatuto ou o seu comportamento[31/32]. A última situação alude ao *resultado*: trata-se de informações que, embora não incidam sobre uma pessoa nem tendam a avaliá-la ou influenciá-la, podem, ainda assim, fazê-lo, isto é, são dados que podem ter um impacto nos direitos e interesses de certa pessoa apesar da ausência dos elementos conteúdo ou finalidade[33/34]. As situações

---

cit., p. 302.

24 WP 29, *Opinion 4/2007* cit., p. 7; e Cordeiro, A. Barreto Menezes, "Dados Pessoais" cit., pp. 302-303.

25 WP 29, *Opinion 4/2007* cit., p. 9; e Cordeiro, A. Barreto Menezes, "Dados Pessoais" cit., p. 303.

26 WP 29, *Opinion 4/2007* cit., p. 9; e Cordeiro, A. Barreto Menezes, "Dados Pessoais" cit., p. 303.

27 Por exemplo, que determinado computador entrou num *site*, que foi efetuada uma chamada de certo telemóvel e a localização de um veículo em circulação.

28 O mesmo raciocínio é aplicável a eventos e a procedimentos onde seja necessária intervenção humana. Cf. WP 29, *Opinion 4/2007* cit., p. 9.

29 WP 29, *Opinion 4/2007* cit., p. 9.

30 WP 29, *Opinion 4/2007* cit., p. 10; e Cordeiro, A. Barreto Menezes, "Dados Pessoais" cit., p. 304.

31 WP 29, *Opinion 4/2007* cit., p. 10; e Cordeiro, A. Barreto Menezes, "Dados Pessoais" cit., p. 304.

32 Considere-se, exemplificativamente, a informação tratada por uma empresa de *marketing* para influenciar o titular dos dados a carregar num anúncio *online*.

33 WP 29, *Opinion 4/2007* cit., p. 11; e Cordeiro, A. Barreto Menezes, "Dados Pessoais" cit., p. 305.

34 Atente-se ao caso de uma empresa de táxis que instala um sistema de localização por

expostas são alternativas e não cumulativas: quando se verificar, por exemplo, a presença do elemento *conteúdo*, não é necessário recorrer à *finalidade* ou ao *resultado*, na medida em que já se pode declarar que a informação é relativa a alguém[35].

Por outro lado, as informações têm de ser relativas a pessoas singulares. Bem evidente desta realidade é o disposto no n.º 1 e 2 do art. 1.º e o Considerando 14 do RGPD, cuja 1ª parte menciona que a proteção conferida pelo Regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência. Excluídos do âmbito do Regulamento estão os dados relativos a pessoas coletivas[36] e a realidades jurídicas não subjetiváveis – fora dos termos explicitados no requisito anterior ("relativa a") –, *maxime* as coisas e os animais[37].

Em último lugar, a informação tem de ser relativa a uma pessoa singular *identificada ou identificável*. Considera-se que a informação é relativa a uma pessoa singular *identificada* se for suficiente para identificar o sujeito de forma inequívoca, sem que sejam necessários dados adicionais[38]. Note-se, todavia, que a determinabilidade ou indeterminabilidade da identidade do titular dos dados dependerá sempre do circunstancialismo da hipótese concreta e do nível de autossuficiência da informação detida[39]. Por sua vez, a informação

satélite para que possa determinar, em tempo real, a posição dos táxis disponíveis. Conquanto a finalidade do tratamento seja fornecer um melhor serviço e conservar combustível, atribuindo a cada cliente que solicite um táxi o veículo que lhe estiver mais próximo, e os dados necessários para o sistema sejam dados relativos aos carros e não aos motoristas, as informações recolhidas permitem avaliar o desempenho destes e verificar, entre outros fatores, se respeitam os limites de velocidade e se procuram os itinerários mais adequados. Nestes termos, os dados podem ser considerados como relativos às pessoas na medida em que podem ter um impacto elevado sobre os motoristas. Cf. WP 29, *Opinion 4/2007* cit., p. 11.

35 WP 29, *Opinion 4/2007* cit., p. 11; e Cordeiro, A. Barreto Menezes, "Dados Pessoais" cit., p. 304.

36 Aduz a 2ª parte do Considerando 14 do RGPD que o Regulamento "[…] não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva". Todavia, diz-nos CORDEIRO, A. Barreto Menezes, "Dados Pessoais" cit., p. 307 que a informação sobre pessoas coletivas pode encontrar-se sujeita ao RGPD quando respeite, direta ou indiretamente, a pessoas singulares – será o caso, por exemplo, em que o nome do sócio ou sócios consta da denominação da pessoa coletiva.

37 Cordeiro, A. Barreto Menezes, "Dados Pessoais" cit., pp. 305-306.

38 WP 29, *Opinion 4/2007* cit., pp. 12-13; e Cordeiro, A. Barreto Menezes, "Dados Pessoais" cit., pp. 311-312.

39 WP 29, *Opinion 4/2007* cit., p. 13; e Cordeiro, A. Barreto Menezes, "Dados

será relativa a uma pessoa *identificável* quando, segundo um critério de razoabilidade, exista a suscetibilidade de o responsável pelo tratamento, ou de um terceiro, conseguir determinar a identidade do titular dos dados pessoais, através da conjugação de informação adicional com a que já detém ou não[40] – isto é o que resulta da correlação entre a 2ª parte do n.º 1 do art. 4.º e o Considerando 26 do RGPD.

Cumpre aclarar que a identificação de uma pessoa não se prende imperativamente com o deslindar do seu nome: basta o recurso a identificadores para distinguir ou isolar alguém dos demais (*single out*)[41]. Cabe aqui chamar a atenção para a tecnologia que, pela sua própria natureza, possibilita rastrear – ou "perseguir" – e observar as pessoas *online*, ou que viabiliza, indiretamente, que estas sejam seguidas e observadas. As pessoas podem ser associadas a identificadores por via eletrónica, fornecidos pelos seus dispositivos, aplicações (*apps*), ferramentas e protocolos – tais como os endereços de IP (*Internet Protocol*) e testemunhos de conexão (*cookies*)[42]. Estes identificadores deixam vestígios que podem ser utilizados para a definição de perfis (*profiling*) e a identificação dos sujeitos, particularmente quando combinados com identificadores únicos e outras informações recebidas pelos servidores[43].

Pegue-se nos *cookies* para ilustrar esta realidade. Os testemunhos de conexão consistem em pequenos ficheiros de texto que são armazenados no computador ou dispositivo móvel dos utilizadores quando estes visitam um *site online*. A funcionalidade dos testemunhos de conexão cinge-se, essencialmente, à monotorização e registo da atividade, comportamentos e outras informações dos cibernautas (como *usernames* e *passwards* para facilitar futuros *logins*, itens adicionados ao carrinho de compras em lojas *online*, hiperligações que foram clicadas anteriormente, quais as páginas *web* mais visitadas, entre muitas outras); para tanto, o *modus operandi* dos *cookies* envolve imputar ao

---

Pessoais" cit., p. 312.

40 WP 29, *Opinion 4/2007* cit., p. 13; e Cordeiro, A. Barreto Menezes, "Dados Pessoais" cit., p. 312.

41 WP 29, *Opinion 4/2007* cit., p. 14; e Leal, Ana Alves, "Aspetos Jurídicos" cit., pp. 108-109.

42 Assim o confirma o Considerando 30 do RGPD.

43 Considerando 30 do RGPD.

utilizador um número ou código exclusivo de forma a identificá-lo[44].

Veja-se que, no domínio do *marketing*, isto consubstancia uma prática enraizada, nomeadamente a propósito do *behavioural targeting* (ou *online profiling*), em que é observada a atividade de alguém na internet como forma a construir o seu perfil – atendendo às suas preferências e aos seus interesses revelados durante a navegação *online* – para que lhe sejam dirigidos anúncios publicitários alusivos a produtos e serviços que se coadunam com o mesmo: conquanto o concreto indivíduo não seja identificado pelo nome, é-lhe imputado um número ou um código único, diferenciando-o dos restantes utilizadores da internet[45]. Deste modo, logra-se construir a personalidade de uma pessoa específica e categorizá-la segundo critérios socioeconómicos, psicológicos, filosóficos ou outros, sendo-lhe posteriormente (ou até mesmo em tempo real) atribuídas certas decisões, baseadas no seu perfil[46].

Em suma, a identificação de uma pessoa não passa, fatalmente, pelo iluminar do seu nome, ou identidade civil[47], bastando diferenciá-la ou isolá-la de todos os demais, o que é possível através dos supramencionados identificadores, que detêm uma ligação próxima e imediata com a pessoa física[48].

IV. O último elemento que compõe o *profiling* é o intento de avaliar certos aspetos pessoais de alguém. O n.º 4 do art. 4.º do RGPD indica que a definição de perfis envolve avaliar determinados fatores pessoais de um sujeito, designadamente analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências, interesses, fiabilidade, comportamento, localização ou deslocações.

Na prática, a definição de perfis envolve com acentuada frequência o recurso a modelos de análise preditiva (*predictive analytics*). Este modelo de análise de dados implica o processo de identificação de padrões a partir

---

44 WP 29, *Opinion 1/2008 on Data Protection Issues Related to Search Engines*, WP 148, Adotado em 4 de abril de 2008, p. 7, disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf.>, consultado a 22 de dezembro de 2021; e Leal, Ana Alves, "Aspetos Jurídicos" cit., p. 108.

45 Leal, Ana Alves, "Aspetos Jurídicos" cit., pp. 107-108.

46 WP 29, *Opinion 4/2007* cit., p. 14.

47 WP 29, *Opinion 4/2007* cit., p. 14; e Leal, Ana Alves, "Aspetos Jurídicos" cit., pp. 108-109.

48 WP 29, *Opinion 4/2007* cit., p. 14.

de conjuntos de dados, de forma a prever resultados, eventos, tendências ou comportamentos futuros; ou seja, após a deteção de padrões relevantes nos dados analisados, associa-se, com base em estatística e probabilidade, esses padrões a determinados resultados, comportamentos, eventos ou tendências futuras[49].

Assim sendo, a definição de perfis envolve a recolha de informações sobre uma pessoa e a avaliação dos seus atributos pessoais ou padrões comportamentais com mira a enquadrá-la em certo grupo ou categoria para, em última instância, prever fatores pessoais seus (como, por exemplo, os seus interesses futuros, sentido de voto nas próximas eleições, a sua capacidade para executar uma futura tarefa ou o presumível cumprimento atempado de obrigações ainda não assumidas)[50].

Todavia, a definição de perfis não implica unicamente que sejam efetuadas previsões futuras sobre as pessoas: de resto resulta este entendimento do próprio n.º 4 do art. 4.º do RGPD quando refere que o objetivo do tratamento automatizado sobre dados pessoais é avaliar elementos pessoais de uma pessoa, nomeadamente *analisar ou prever* aspetos específicos (considere-se, exemplificativamente, a análise da situação económica ou do estado de saúde do titular dos dados).

De qualquer modo, o que decorre deste terceiro elemento é que não se revela satisfatória a organização ou estruturação dos dados pessoais recolhidos, isto é, não consubstancia uma definição de perfis a mera categorização de pessoas atendendo a concretas qualidades ou características (*v.g.* idade, sexo e altura)[51]. O vocábulo "avaliar" presente no n.º 4 do art. 4.º do RGPD conduz à tese de que o *profiling* pede algo mais do que a simples catalogação: postula a existência de qualquer tipo de apreciação ou juízo sobre uma pessoa[52/53].

---

49 Leal, Ana Alves, "Aspetos Jurídicos" cit., pp. 82-83.

50 WP 29, *Guidelines* cit., p. 7.

51 WP 29, *Guidelines* cit., p. 7; e Cordeiro, A. Barreto Menezes, *Direito* cit., p. 149.

52 WP 29, *Guidelines* cit., p. 7; e Cordeiro, A. Barreto Menezes, *Direito* cit., p. 149.

53 Desde modo, se uma empresa tenciona classificar os seus clientes atendendo à idade destes, com finalidades, tão-só, estatísticas e para ter uma visão geral agregada daqueles, sem tirar ilações ou efetuar quaisquer previsões, então a utilidade não é apreciar as características individuais dos clientes, pelo que não se está no campo do *profiling*, por faltar o último elemento caracterizador da figura. Cf. WP 29, *Guidelines* cit., p. 7.

3. Perigos Intrínsecos à Definição de Perfis

I. Conquanto o *profiling* consubstancie uma mais-valia para os indivíduos, organizações e para a própria comunidade de um modo geral[54], não deixa de ser uma atividade concatenada com riscos que não devem ser observados com desmazelo e leviandade. Nestes termos, a tutela atribuída ao titular dos dados perante a definição de perfis encontra a sua fundamentação na perniciosidade subjacente a esta subcategoria de tratamento de dados pessoais.

i) Um maleficio sisudo proveniente da definição de perfis, que tende a passar despercebido aos próprios titulares dos dados, é a criação de novos dados decorrente da categorização de um sujeito[55]. O *profiling*, mais do que identificar as pessoas que se inserem num concreto grupo, potencializa, através das técnicas, correlações e inferências aplicadas, a descoberta de atributos específicos de um indivíduo que este não transmitiu diretamente ou deduz não serem conhecidos[56].

Através da combinação e interligação de dados, existe até a possibilidade de serem obtidos ou inferidos dados sensíveis (também apelidados de dados especiais) a partir de preferências e atributos que não o são[57], ou seja, decorrente da interligação de *non-sensitive data* (ou "*harmless information*"[58])[59]. Embora o Regulamento não forneça um conceito de dados sensíveis, o RGPD elenca taxativamente[60] os dados que lhe integram, dispondo o n.º 1 do art. 9.º que "é proibido o tratamento de dados pessoais que revelem

54 Como forma a esclarecer alguns dos benefícios associados a este tratamento de dados observe-se o que sucede no domínio da comercialização de produtos e serviços: a definição de perfis possibilita segmentar melhor os mercados e adequar os bens e serviços às necessidades individuais dos consumidores, bem como calcular os seus custos em função das características e categorias de pessoas, designadamente do seu poder de compra. Cf. CoE, *The Protection* cit., pp. 6 e 41, para. 108; e WP 29, *Guidelines* cit., p. 5.

55 CoE, *The Protection* cit., pp. 6 e 28, para. 50.

56 CoE, *The Protection* cit., pp. 6 e 28, para. 50; e WP 29, *Guidelines* cit., p. 9.

57 CoE, *The Protection* cit., p. 25, para. 37, e p. 31, para. 61; e WP 29, *Guidelines* cit., p. 15.

58 Esta expressão é utilizada em CoE, *The Protection* cit., p. 25, para. 37 para designar os dados pessoais não pertencentes às categorias de dados sensíveis.

59 Por exemplo, é possível inferir o estado de saúde de uma pessoa articulando os registos das suas compras de produtos alimentares com informações concernentes com a qualidade e o valor energético daqueles alimentos. Cf. WP 29, *Guidelines* cit., p. 15.

60 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 133.

a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos[61], dados biométricos[62] para identificar uma pessoa de forma inequívoca, dados relativos à saúde[63] ou dados relativos à vida sexual ou orientação sexual de uma pessoa". Os dados especiais consistem numa modalidade de dados que são, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, uma vez que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais do titular[64].

Os cuidados peculiares a ter com os dados sensíveis justificam-se por quatro ordens de razão: *(i)* pelo princípio da não discriminação – plasmado, entre outros locais, no n.º 1 do art. 21.º da Carta dos Direitos Fundamentais da União Europeia –; *(ii)* pela natureza de direito fundamental detida pela grande parte dos dados apresentados; *(iii)* pela situação de vulnerabilidade em que se encontra, em algumas das situações, o titular dos dados – pense-se nos dados relativos à saúde –; *(iv)* ou pelos efeitos nocivos que podem advir do seu tratamento[65]. No fundo, consubstanciam dados com um cariz marcadamente pessoal[66].

Por outro lado, a integração de uma pessoa numa certa categoria significa necessariamente serem-lhe, também, atribuídas outras informações derivadas daquele grupo, embora só sejam com ele partilhadas determinadas características, criando-se, desta forma, novos dados relativamente àquele sujeito[67/68]. Tipicamente, o titular dos dados não suspeita – nem o poderia

61 *Vide* o n.º 13 do art. 4.º do Regulamento.

62 *Vide* o n.º 14 do art. 4.º do Regulamento.

63 *Vide* o n.º 15 do art. 4.º, bem como o Considerando 35 do Regulamento.

64 Considerando 51 do RGPD.

65 Com este entendimento, Cordeiro, A. Barreto Menezes, *Direito* cit., p. 133, que menciona, com igualdade, o dissenso em torno destes fundamentos, existindo quem considere que o critério para integrar certos dados nesta categoria especial é turvo e puramente arbitrário.

66 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 133.

67 CoE, *The Protection* cit., pp. 28-29, para. 53.

68 Pegando num exemplo com a análise preditiva (*predictive analytics*): se se prevê que os sujeitos que são parte de uma categoria, por partilharem as características A e B, com elevada probabilidade, interessar-se-ão futuramente por um novo produto (característica C), então a pessoa que tem as qualidades A e B também é dotada da característica C. Recorrendo a outro caso: se uma instituição de crédito deteta que as pessoas pertencentes ao grupo com os atributos D e E têm graves dificuldades em cumprir as suas obrigações pecuniárias (qualidade

fazer atendendo à magnitude e complexidade do processo – das correlações que decorrem nem dos resultados a que estas conduzem.

ii) Importa reiterar que uma parte nuclear do *profiling* apoia-se na estatística e na probabilidade[69]. Efetivamente, os perfis são padrões oriundos de um processamento estatístico e probabilístico da informação recolhida, pelo que não espelham infalivelmente a realidade, mas, tão-só, uma versão desta assente no processo de análise de dados efetuado[70]. Enquanto tal, uma consequência inevitável é a incerteza em torno do resultado a que conduz o procedimento técnico *sub oculis*[71]. Existem dois erros suscetíveis de ocorrer com a definição de perfis: a introdução errónea de um sujeito em certo grupo (falsos positivos), sendo-lhe, assim, atribuído características erradas, e a exclusão de alguém de um grupo a que efetivamente pertence (falsos negativos)[72/73].

Isto pode suceder, por um lado, por os dados recolhidos serem inexatos: as decisões ou os perfis fundados em dados desatualizados – contando que não se tratem de dados que apenas têm interesse num estado desatualizado por dizerem respeito a realidades passadas (por exemplo, dados médicos que descrevem um estado clínico antigo)[74] – ou incorretos serão forçosamente imprecisos, conduzindo a previsões ou declarações inadequadas e desacertadas em relação ao sujeito visado[75]. Por outro lado, mesmo que os dados a analisar sejam corretos, podem não ser suficientemente representativos – por não terem sido obtidos todos os dados que relevam para a construção do perfil – ou os algoritmos podem conter enviesamentos humanos ocultos (*hidden bias*)[76], tais

F) então muito provavelmente será recusada a concessão de crédito a alguém que tenha as características D e E por lhe ser imputada a qualidade F.

69 Oliveira, Madalena Perestrelo de, "Definição de Perfis" cit., p. 68; e CoE, *The Protection* cit., p. 29, para. 54, e p. 39, para. 97.

70 Oliveira, Madalena Perestrelo de, "Definição de Perfis" cit., p. 69.

71 CoE, *The Protection* cit., pp. 6 e 29; e WP 29, *Guidelines* cit., p. 6.

72 CoE, *The Protection* cit., p. 29, para. 54.

73 Tome-se como exemplo certos clientes de uma instituição de crédito, considerados como indesejáveis por o perfil traçado estar associado a um grupo com um elevado risco de incumprimento, quando na realidade não é isto que se verificaria; ou os clientes a quem é concedido um crédito, por se enquadrarem numa categoria com conotações positivas, quando de facto não cumpriram atempadamente as suas obrigações. Cf. CoE, *The Protection* cit., p. 29, para. 54.

74 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 159.

75 WP 29, *Guidelines* cit., p. 12.

76 Oliveira, Madalena Perestrelo de. "Definição de Perfis" cit., p. 69; e WP 29,

como critérios discriminatórios.

iii) Enquanto efeitos colaterais da identificação de perfis que se inserem numa concreta categoria ou grupo aponta-se, ainda, a suscetível estigmatização, através da perpetuação de estereótipos existentes, e a segregação social[77].

A definição de perfis comporta um verdadeiro potencial discriminatório, possibilitando a negação, injustificada, de bens e serviços a certos grupos de pessoas com base na sua origem racial ou étnica, estatuto económico, idade, género, orientação sexual, convicções religiosas ou por padecerem de quaisquer deficiências, entre muitos outros fatores[78]. É imperativo mencionar que nem todo o tratamento desigual representa uma discriminação: o exercício da definição de perfis implica, pela sua própria natureza, uma distinção entre utilizadores, clientes, consumidores e cidadãos, visando um tratamento não igualitário entre eles[79]. O que não pode ser aceite é um tratamento diferenciado arbitrário, sem nenhum motivo aparente ou apoiado em justificações que não sejam razoáveis e que atentem contra o princípio da igualdade[80].

De qualquer modo, é inegável que esta categorização limita, no fundo, as pessoas às preferências sugeridas, produzindo, enquanto tal, impactos na sua liberdade de escolha relativamente a determinados produtos ou serviços (*v.g.*, serem recomendados certos filmes e séries, músicas e livros em detrimento de outros; ou serem propostos certos fluxos de notícias e ocultados outros)[81].

iv) Um dos métodos através do qual é possível criar perfis é com recurso à pegada digital que os cibernautas deixam ao navegarem pela internet. Através da atividade de alguém *online* (como os vídeos e as imagens visualizadas, as fotografias publicadas, as notícias e os *tweets* partilhados, as páginas *web* visitadas e os *likes* nas redes sociais) é possível obter-se, entre outros aspetos pessoais, as suas características psicológicas[82]. Nestes termos, vigora um real perigo de persuasão psicológica e manipulação em massa, uma vez detetado

---

Guidelines cit., p. 12.

77 WP 29, *Guidelines* cit., p. 5.

78 CoE, *The Protection* cit., pp. 6-7; e WP 29, *Guidelines* cit., p. 6.

79 CoE, *The Protection* cit., p. 41, para. 108.

80 CoE, *The Protection* cit., p. 41, paras. 106-107.

81 WP 29, *Guidelines* cit., pp. 5-6.

82 Matz, S. C. , Kosinski, M. , Nave, G. , Stillwell, D. J., "Psychological Targeting as an Effective Approach to Digital Mass Persuasion", *Proceedings of the National Academy of Sciences*, 114, 48, 2017, pp. 12714-12719, p. 12714.

um grupo de pessoas que seja facilmente influenciável[83].

As investigações têm deslindado que adaptar o conteúdo dos anúncios às qualidades psicológicas de certas pessoas, particularmente daquelas mais vulneráveis, é uma operação suscetível de modificar amplamente o comportamento daqueles sujeitos[84]. Conquanto a influência possa ser benéfica para as próprias pessoas (como persuadir um grupo com maus hábitos alimentares a ter uma alimentação saudável), ela pode também, em contrariedade, seguir um sentido perverso (tal como convencer uma categoria de pessoas facilmente viciáveis a participar em jogos de azar[85] ou manipulá-las a votar em certo sentido através da distorção da sua perceção da realidade).

Entretanto, importa notar que, em qualquer dos casos, independentemente da índole dos seus resultados, a persuasão pode configurar-se deletéria, porquanto, com ou sem consequências benéficas, a manipulação pode ser percecionada como algo intrusivo, por parte do titular dos dados.

II. Os perigos em torno do *profiling* pintam um quadro estarrecedor da vulnerabilidade e fragilidade suscetível de pairar sobre as pessoas. Alicerçadas nestas justas preocupações, as instituições da União Europeia sentiram-se compelidas a realçar no Considerando 72 do RGPD que a definição de perfis está subjugada às regras que regem o tratamento de dados pessoais, entre as quais a licitude do tratamento (art. 6.º) e os princípios da proteção de dados (art. 5.º).

4. Direito de Oposição

I. O Regulamento confere ao titular dos dados certos instrumentos de autodefesa que possibilitam a sua reação quando o tratamento comporte elevados riscos ou seja indesejado[86], entre estes consta o direito de oposição.

Proclama o Regulamento que o titular dos dados tem o direito de se opor

83 Matz, S. C. , Kosinski, M., Nave, G., Stillwell, D. J., "Psychological Targeting" cit., p. 12714.

84 Matz, S. C., Kosinski, M., Nave, G., Stillwell, D. J., "Psychological Targeting" cit., p. 12715.

85 Matz, S. C., Kosinski, M., Nave, G., Stillwell, D. J., "Psychological Targeting" cit., p. 12714.

86 Leal, Ana Alves, "Aspetos Jurídicos" cit., pp. 122-123.

à definição de perfis (art. 21.º, n.º 1, do RGPD)[87/88]. Contudo, não se trata de um poder de exercício livre, tendo o titular de o fundamentar através de razões relacionadas com a sua situação particular (art. 21.º, n.º 1, do RGPD). Segundo o que resulta da 2ª parte do n.º 1 do art. 21.º do RGPD, a situação particular do titular dos dados andará concatenada com os seus direitos e liberdades ou interesses[89] (de índole pessoal, social ou profissional[90]). Encontra-se, assim, positivada uma solução ampla e casuística, cabendo apenas ao titular ser claro e preciso nos motivos que apresenta para a não realização do processo de *profiling*[91].

Todavia, nos termos do n.º 1 do art. 21.º do RGPD, ainda que devidamente justificado, o direito de oposição apenas pode ser invocado perante um número circunscrito de situações: quando o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento (art. 6.º, n.º 1, al. e*)* do RGPD); e quando o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros (art. 6.º, n.º 1, al. f*)* do RGPD)[92].

O n.º 1 do art. 21.º do RGPD também menciona as hipóteses em que o tratamento é realizado para fins diferentes daqueles para os quais os dados tenham sido recolhidos (art. 6.º, n.º 4, do RGPD), ou seja, à partida, o direito

87 O direito de oposição é um corolário da natureza pessoal do direito à autodeterminação informacional – cf. Cordeiro, A. Barreto Menezes, *Direito* cit., p. 299 –, que concede a cada um o direito de controlar, em todas as fases do tratamento, a informação disponível a seu respeito, impedindo que a pessoa se transforme num simples objeto de informações ou num produto – cf. Canotilho, J. J. Gomes, Moreira, Vital, *Constituição da República Portuguesa Anotada*, I, 4ª Edição, Coimbra Editora, 2007, p. 551; e Leal, Ana Alves, "Aspetos Jurídicos" cit., p. 124.

88 A menção direta à definição de perfis no n.º 1 do art. 21.º do RGPD pode ser tida como dispensável, no sentido de que a sua omissão não removeria o direito do titular dos dados a opor-se à definição de perfis nos contextos traçados, permanecendo a norma aplicável em tais circunstâncias. Simplesmente, visa-se chamar a atenção (e bem!) para estes casos mais melindrosos. Cf. Cordeiro, A. Barreto Menezes, *Direito* cit., p. 302.

89 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 301.

90 WP 29, *Guidelines* cit., p. 19.

91 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 301.

92 A existência de interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros não basta para fundar um tratamento lícito: há que levar a cabo um teste de ponderação, confrontando o peso que assumem *in casu* os interesses legítimos do responsável ou de terceiros e os interesses, direitos e liberdades do titular (art. 6.º, n.º 1, al. f*)*, do RGPD).

de oposição pode operar quando os dados pessoais forem reutilizados para a prática de novas operações de tratamento, entre as quais se localiza o *profiling*. No entanto, a referência feita ao n.º 4 do art. 6.º do RGPD pelo n.º 1 do art. 21.º do RGPD deve ser ignorada, por se tratar de um erro, não constando aquela menção nos correspondentes artigos das demais versões do Regulamento[93].

Nesta senda, o direito em apreço possibilita que o titular se oponha ao tratamento lícito dos seus dados pessoais[94]. Pode-se apontar uma tripla justificação para esta realidade.

Desde logo, em contrariedade aos demais fundamentos jurídicos, que colocam o titular em primeiro plano, sustentando-se no seu direito à autodeterminação informacional e nos seus interesses, os fundamentos de licitude para o tratamento de dados pessoais contemplados nas alíneas e*)* e f*)* do n.º 1 do art. 6.º do RGPD visam prosseguir interesses de terceiros (individuais ou coletivos)[95].

Entre todas as exclusões, merece ser destacado que fora do campo de incidência deste direito encontram-se as situações em que o titular tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas (art. 6.º, n.º 1, al. a*)* do RGPD). Sendo o consentimento do titular o exponente máximo do controlo dos dados e, como tal, do princípio da autodeterminação informacional[96], para os casos em que o titular não haja previsto todas as consequências que decorrem do seu consentimento, não tenha antecipado eventuais e prováveis evoluções tecnológicas que permitem ao responsável pelo tratamento retirar dos seus dados pessoais mais informações do que o titular esteja disposto a partilhar ou, tão-só, quando o titular pretenda voltar atrás por ter alterado subjetivamente a sua opinião, o n.º 3 do art. 7.º do RGPD reserva o direito à revogação do consentimento[97].

Em segundo lugar, atendendo às particularidades dos fundamentos jurídicos indicados no n.º 1 do art. 21.º do RGPD, é possível que uma decisão

93 Fidalgo, Vítor Palmela, "Artigo 21.º" *in* Cordeiro, A. Barreto Menezes (Coord.), *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Almedina, 2021, pp. 213-220, p. 217.

94 Considerando 69 do RGPD.

95 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 301.

96 Leal, Ana Alves, "Aspetos Jurídicos" cit., p. 150.

97 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 188.

seja tomada, pelo responsável pelo tratamento, com desconhecimento da particular situação em que se encontra o titular dos dados; o direito de oposição, nos contornos em que foi traçado, viabiliza que o titular dê a conhecer ao responsável pelo tratamento a dita situação especial[98].

Por último, estender o direito de oposição a outros fundamentos de licitude seria, em certas circunstâncias, gerador de uma verdadeira inconsistência de um prisma dogmático: o exercício do direito de oposição no contexto da execução de um contrato (art. 6.º, n.º 1, al. b*)*, do RGPD) representaria um abuso de direito, *in concreto* o tipo *venire contra factum proprium*, e quando o tratamento fosse necessário para o cumprimento de uma obrigação legal a que o responsável pelo tratamento estivesse sujeito (art. 6.º, n.º 1, al. c*)*, do RGPD), prevaleceria sempre a Lei sobre a vontade do titular dos dados[99].

Com tudo isto, torna-se patente as razões particulares que motivam a contenção do direito de oposição às circunstâncias indicadas no n.º 1 do art. 21.º do RGPD, não se admitindo a sua extensão aos demais fundamentos de licitude.

Ademais, o direito de oposição obedece, numa primeira fase, a uma lógica potestativa: "a constituição [deste direito] (em sentido técnico-jurídico) na esfera do titular dos dados depende de prévia declaração unilateral deste, dirigida ao responsável pelo tratamento; só então este, na posição passiva, passa a estar adstrito ao *dever* de […] cessar o […] tratamento [dos dados pessoais]. A mecânica potestativa que antecede a constituição [deste direito] permite antever que em causa [está um meio de defesa] do titular dos dados *também* perante condutas lícitas do responsável pelo tratamento; é que, de outra forma, sendo o tratamento proibido, e em contraste com este funcionamento potestativo, o responsável pelo tratamento estaria já (independentemente de qualquer impulso de defesa por parte do titular dos dados) obrigado a não praticar nenhum comportamento tendente a esse tratamento. Por isso, nesses casos, e diferentemente do que aqui se analisa, conta-se com o binómio «direito/dever» desde o início, sem que seja precedido pelo binómio «poder/sujeição»"[100].

98 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 301.
99 Cordeiro, A. Barreto Menezes, *Direito* cit., pp. 301-302.
100 Leal, Ana Alves, "Aspetos Jurídicos" cit., p. 133.

Opondo-se o titular dos dados ao *profiling*, o responsável pelo tratamento tem de interromper o processo de definição de perfis ou evitar o seu começo, até se verificar, sendo esse o caso, que existem motivos legítimos do responsável pelo tratamento prevalecentes sobre os interesses, os direitos e as liberdades do titular dos dados (art. 18.º, n.º 1, al. d*)*, do RGPD)[101].

II. Sem prejuízo da limitação do tratamento, os dois requisitos cumulativos anunciados – o tratamento se fundar na alínea e*)* ou f*)* do n.º 1 do art. 6.º do RGPD e o titular conjurar motivos relacionados com a sua situação particular – não bastam por si só para que imperativamente cesse o tratamento *sub oculis*. Perante o exercício do direito de oposição, o responsável pelo tratamento deve analisar o pedido feito pelo titular[102] e cessar o tratamento, exceto *(i)* se apresentar razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou *(ii)* se o tratamento for necessário para efeitos de declaração, exercício ou defesa de um direito num processo judicial (art. 21.º, n.º 1, 2ª parte, do RGPD).

O Regulamento não clarifica o que se deve entender por "razões imperiosas e legítimas". Não obstante, os tratamentos a que o titular se pode opor – aqueles a que alude as alíneas e*)* e f*)* do n.º 1 do art. 6.º *ex vi* n.º 1 do art. 21.º do RGPD – apontam no sentido de que a expressão "razões legítimas" engloba quer interesses do próprio responsável, quer interesses de terceiros[103]. No que concerne ao vocábulo "imperioso", este aparenta incutir a ideia de que as razões legítimas devem posicionar-se num limiar mais elevado do que os interesses, direitos e liberdades declarados pelo titular dos dados, de modo a prevalecer sobre estes[104/105].

O responsável pelo tratamento tem, deste modo, de cumprir um exigente

101 WP 29, *Guidelines* cit., p. 18.

102 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 302.

103 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 303.

104 WP 29, *Guidelines* cit., p. 19.

105 WP 29, *Guidelines* cit., p. 18 retrata, exemplificativamente, uma razão imperiosa e legítima, indicado o caso em que a definição de perfis serve para prever a propagação de doenças contagiosas. Com efeito, para além de outros contextos, existem razões legítimas e imperiosas nas situações em que a definição de perfis acarreta vantagens para a sociedade como um todo ou para a comunidade em geral.

exercício de ponderação[106], onde é considerada a significância do *profiling* para o seu objetivo específico, o impacto da definição de perfis sobre os interesses, os direitos e as liberdades do titular dos dados – devendo o *profiling* ser limitado ao mínimo necessário para atingir a finalidade visada, isto é, ser o menos intrusivo possível – e a medida da prevalência das razões imperiosas e legítimas sobre os interesses, direitos e liberdades do titular dos dados[107].

Compete, assim, ao responsável pelo tratamento provar que os seus interesses legítimos imperiosos prevalecem sobre os interesses ou direitos e liberdades do titular dos dados, de modo a justificar a definição de perfis[108/109]. Em caso de dúvida, prevalecerá a posição do titular dos dados, devendo o responsável pelo tratamento cessar o mesmo[110].

III. Uma vez invocada a oposição e devidamente justificada pelo titular dos dados e não sendo o seu exercício obstaculizado com base na 2ª parte do n.º 1 do art. 21.º do RGPD, o responsável pelo tratamento deve cessar o processo de *profiling* (art. 21.º, n.º 1, do RGPD) e, mediante pedido apresentado pelo titular, eliminar, sem demora injustificada, os dados pessoais utilizados para criar o perfil, bem como o próprio perfil[111] (art. 17.º, n.º 1, al. c*)*, do RGPD). Em contrariedade, verificando-se que os motivos legítimos do responsável prevalecem sobre os do titular dos dados, é anulada a limitação que foi implementada ao referido tratamento, nos termos da al. d*)* do n.º 1 do art. 18.º do RGPD, quando este último manifestou a sua oposição. Nesta eventualidade, o titular deve ser informado previamente à dita anulação que a limitação do tratamento vai ser, precisamente, anulada porque os motivos legítimos do responsável pelo tratamento prevalecem sobre os seus (art. 18.º, n.º 3, do RGPD).

---

106 WP 29, *Guidelines* cit., p. 19; e LEAL, Ana Alves, "Aspetos Jurídicos" cit., p. 134.

107 WP 29, *Guidelines* cit., pp. 18-19.

108 Considerando 69 do RGPD.

109 Evidencia-se, desta forma, que o teste de ponderação imposto pelo n.º 1 do art. 21.º do RGPD é diferente daquele que resulta da alínea f*)* do n.º 1 do art. 6.º do RGPD: não basta que o responsável demonstre que os interesses, direitos ou liberdades fundamentais do titular não prevaleceram sobre os seus interesses legítimos, mas que estes são, também, imperiosos. Cf. WP 29, *Guidelines* cit., p. 19.

110 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 303.

111 WP 29, *Guidelines* cit., p. 18.

O direito de oposição pode ser exercido em qualquer momento (art. 21.º, n.º 1, do RGPD). Contudo, esta referência temporal deve ser entendida como antes do tratamento ou na sua pendência, não podendo o mencionado direito ser invocado após o término do tratamento[112], pois, se este já transcorreu, a oposição perde o seu sentido. Por outro lado, a oposição por parte do titular apenas opera para o futuro: o direito de oposição não tem efeitos retroativos[113].

IV. O titular pode, talqualmente, opor-se ao tratamento dos seus dados pessoais quando estes estejam a ser tratados para efeitos de comercialização direta (art. 21.º, n.º 2, do RGPD). O direito de oposição relativo ao *marketing* direto abrange também a definição de perfis, na medida em que esteja relacionada com aquela comercialização (art. 21.º, n.º 2, *in fine*, do RGPD).

O direito assume *in casu* uma dimensão incondicional: não é necessário efetuar qualquer ponderação de interesses, devendo o responsável pelo tratamento respeitar a vontade do titular sem questionar os motivos subjacentes à oposição[114]. Assim, não é necessário de ser invocado qualquer argumento substantivo, sendo suficiente para possibilitar o exercício do direito em apreço o mero facto de os dados pessoais serem utilizados para efeitos de comercialização direta[115].

Sempre que os dados pessoais sejam objeto de tratamento para o mencionado fim, o titular pode opor-se a qualquer momento (art. 21.º, n.º 2, do RGPD), de forma gratuita, independentemente de se tratar do tratamento inicial ou do tratamento posterior[116]. Ora, preceitua a 1ª parte do n.º 2 do art. 12.º do RGPD que o responsável pelo tratamento deve facilitar o exercício dos direitos atribuídos ao titular dos dados. Daqui se retira que os responsáveis pelo tratamento, que recolhem dados pessoais junto dos seus titulares com o propósito de os utilizar para efeitos de comercialização direta, devem, aquando da recolha, considerar facultar aos titulares meios fáceis para que estes assinalem naquele momento que não desejam que os seus dados sejam

112 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 302.

113 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 302.

114 Cordeiro, Madalena Perestrelo de, "Definição de Perfis" cit., p. 72; e WP 29, *Guidelines* cit., p. 19.

115 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 303.

116 Considerando 70 do RGPD.

objeto do referido tratamento, invés de os "forçar" a ter que exercer o seu direito de oposição num momento porvindouro[117]. De qualquer modo, isto não expressa uma obrigatoriedade, mas uma forma concebível de facilitar ao titular dos dados o exercício do direito em questão.

Uma vez invocada a oposição ao tratamento para efeitos de comercialização direta pelo titular, os dados deixam de ser tratados para esse fim (art. 21.º, n.º 3, do RGPD). Acrescenta a al. c*)* do n.º 1 do art. 17.º do RGPD que o responsável pelo tratamento pode encontra-se ainda adstrito a ter que apagar os dados pessoais em causa e o perfil criado[118], sem demora injustificada, se o titular assim o requerer.

Embora observados os contornos deste regime subsiste a dúvida do que se deve entender por "comercialização direta". O Regulamento não fornece qualquer definição desta expressão e o mesmo se diga quanto ao Direito da União Europeia. Ainda assim, a Comissão Europeia afirma que a comercialização direta corresponde a "qualquer ação, por parte de uma empresa, destinada a comunicar material publicitário ou de comercialização, dirigida a pessoas específicas"[119]. Um indício do conceito também pode ser encontrado na Proposta de Regulamento relativo à privacidade e às comunicações eletrónicas[120], cuja alínea f*)* do n.º 3 do art. 4.º define como sendo comunicações comerciais diretas "qualquer forma de publicidade, oral ou escrita, enviada a um ou mais utilizadores finais identificados ou identificáveis de serviços de comunicações eletrónicas, incluindo a utilização de sistemas de chamada e de comunicação automatizados, com ou sem interação humana, de correio eletrónico, SMS, etc.". Por seu turno, nos termos da alínea a*)* do art. 2.º da Diretiva 2006/114/CE do Parlamento Europeu e do Conselho, de 12 de dezembro de 2006, relativa à publicidade enganosa e comparativa, por publicidade entende-se "qualquer

117 WP 29, *Guidelines* cit., p. 19, nota n.º 31.

118 WP 29, *Guidelines* cit., p. 18.

119Cf.<https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/what-happens-if-someone-objects-my-company-processing-their-personal-data_en>, consultado a 22 de dezembro de 2021.

120 European Comission, Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final – 2017/0003 (COD), 10 January 2017, disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN>, consultado a 22 de dezembro de 2021.

forma de comunicação feita no âmbito de uma atividade negocial, comercial, artesanal ou liberal com o objetivo de promover o fornecimento de bens ou de serviços, incluindo bens imóveis, direitos e obrigações".

Estes conceitos tornam evidentes que a comercialização direta, a que alude o n.º 2 do art. 21.º do RGPD, assume um cariz comercial. O direito de oposição pode ser livremente exercido quando a oposição se reporta ao tratamento de dados pessoais para efeitos de comercialização direta com índole comercial[121].

De facto, a letra do n.º 2 do art. 21.º do RGPD não especifica a natureza da comercialização direta, o que tem levado uma fação doutrinária a sufragar o entendimento de que o direito de oposição vale contra todos os tipos de comercialização direta, quer detenha propósitos comerciais, políticos, religiosos ou de qualquer outra natureza[122]. Porém, a aplicação prática do n.º 2 do art. 21.º do RGPD revela como esta posição não é merecedora de colhimento: pegando num exemplo em que o tratamento dos dados pessoais é necessário para o exercício de funções de interesse público (art. 6.º, n.º 1, al. e*)*, do RGPD) e a comercialização direta visa informar os cidadãos de uma determinada ocorrência ou perigo, o titular poderia *in casu* opor-se incondicionalmente a esta comercialização, pois, em contrariedade ao n.º 1 do art. 21.º do RGPD, o n.º 2 do art. 21.º do RGPD não envolve a avaliação dos interesses em confronto[123]. Uma interpretação literal do n.º 2 do art. 21.º do RGPD patenteia-se, assim, desajustada face aos distintos contornos com que o direito de oposição foi desenhado no n.º 1 e 2 do art. 21.º do RGPD.

V. O dever de informar o titular dos dados sobre a existência do direito de oposição é algo que decorre, desde logo, da alínea b*)* do n.º 2 do art. 13.º do RGPD, quando os dados sejam recolhidos junto do titular, e da alínea c*)* do n.º 2 do art. 14.º do RGPD, quando os dados não sejam recolhidos juntos do

121 Em sentido coincidente, Cordeiro, A. Barreto Menezes, *Direito* cit., p. 305.

122 Cordeiro, A. Barreto Menezes, *Direito* cit., pp. 304-305 dá nota da cisão presente na Ciência Jurídica alemã, alicerçada nas duas posições apresentadas, isto é, na interpretação literal, que admite o direito de oposição face a todos os tipos de comercialização direta, e na interpretação restritiva com base teológica, que delimita o direito de oposição ao campo da comercialização direta com intuitos comerciais.

123 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 305.

titular. Não obstante, elabora o n.º 4 do art. 21.º do RGPD que o responsável pelo tratamento deve, o mais tardar no momento da primeira comunicação ao titular dos dados, informar explicitamente este último sobre o direito de oposição plasmado no n.º 1 e 2 do art. 21.º do RGPD, apresentando-o de modo claro e distinto de quaisquer outras informações. Enquanto tal, a indicação deste direito não pode ser ocultada ou dissimulada nos termos e condições que são apresentadas ao utilizador, devendo o direito ser destacado num documento relevante ou no respetivo *website* do responsável pelo tratamento[124]. Atente-se que da menção expressa ao n.º 2 do art. 21.º do RGPD resulta que, se porventura, a definição de perfis se destinar ao *marketing* direto, deve isto ser levado ao conhecimento do titular (art. 13.º, n.º 1, al. c*)*, e art. 14.º, n.º 1, al. c*)*, do RGPD) para que este opte ou não por exercer o direito de oposição, precisamente, nos termos do n.º 2 do art. 21.º do RGPD.

Noutra senda, o Regulamento não determina uma forma concreta para o exercício do direito de oposição por parte do titular, podendo ser por escrito ou oralmente[125]. Sem prejuízo disto, no âmbito dos serviços da sociedade da informação, aquele direito pode ser exercido por meios automatizados, utilizando especificações técnicas (art. 21.º, n.º 5, do RGPD) – *v.g.* através do recurso a ferramentas que possibilitam bloquear o rastreamento do comportamento *online* do cibernauta[126]. O n.º 25 do art. 4.º do RGPD remete a definição de serviço da sociedade da informação para a noção de serviço apresentada na al. b*)* do n.º 1 do art. 1.º da Diretiva 2015/1535, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação: "«serviço» significa qualquer serviço da sociedade da informação, isto é, qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços".

---

124 WP 29, *Guidelines* cit., p. 32.

125 Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)*, 02 de agosto de 2018, p. 143, disponível em <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>, consultado a 22 de dezembro de 2021.

126 Jef Ausloos, The Interaction Between the Rights to Object and to Erasure in the GDPR, 2016, disponível em: <https://www.law.kuleuven.be/citip/blog/gdpr-update-the-interaction-between-the-right-to-object-and-the-right-to-erasure>, consultado a 22 de dezembro de 2021.

O conceito de serviço da sociedade da informação pode assim ser decomposto em cinco elementos caracterizadores[127]: *(i)* trata-se de uma prestação; *(ii)* normalmente remunerada; *(iii)* realizada à distância; *(iv)* por via eletrónica; e *(v)* mediante pedido individual do destinatário do serviço. Apenas colhem valor, para efeitos da noção levantada, as *prestações* principais: as "prestações que desempenhem um papel secundário ou não nuclear no serviço efetivamente prestado não são relevadas"[128]. A *remuneração* não tem de possuir um cariz monetário, nem a contraprestação tem de ser suportada pelo beneficiário, bastando que se trate de uma relação comercial *lato sensu*[129/130]. A prestação é *realizada à distância* quando o serviço é prestado sem que as partes estejam simultaneamente presentes (art. 1.º, n.º 1, al. b*)*, i*)* da Diretiva 2015/1535, de 9 de setembro de 2015), não obtendo a qualificação de serviço da sociedade da informação os serviços prestados na presença física do prestador e do destinatário, mesmo que impliquem a utilização de dispositivos eletrónicos[131]. O serviço prestado *por via eletrónica* corresponde ao serviço enviado desde a origem e recebido no destino através de instrumentos eletrónicos de processamento (incluindo a compressão digital) e de armazenamento de dados, que é inteiramente transmitido, encaminhado e recebido por cabo, rádio, meios óticos ou outros meios eletromagnéticos (art. 1.º, n.º 1, al. b*)*, ii*)* da Diretiva 2015/1535, de 9 de setembro de 2015). Não são, assim, serviços fornecidos por via eletrónica os serviços cujo conteúdo é material mesmo quando impliquem a utilização de dispositivos eletrónicos, os serviços *offline* e os serviços não fornecidos por intermédio de sistemas eletrónicos de armazenagem e processamento de dados[132]. Por fim, a expressão "*mediante pedido individual do destinatário do serviço*" reporta-se a um

127 Cordeiro, A. Barreto Menezes, Direito cit., pp. 197-198

128 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 197.

129 Cordeiro, A. Barreto Menezes, *Direito* cit., p. 197.

130 É o que se verifica, por exemplo, com os motores de busca online, as redes sociais e com muitas das apps, cuja remuneração não deriva diretamente do utilizador, mas, antes, dos anúncios exibidos; e com os sites e jogos online educacionais, que, embora não tenham fins lucrativos, podem ser considerados como uma atividade econômica em sentido amplo, na medida em que são tipos de serviços normalmente prestados num campo comercial – cf. <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/>, consultado a 22 de dezembro de 2021.

131 Anexo I da Diretiva 2015/1535, de 9 de setembro de 2015.

132 Anexo I da Diretiva 2015/1535, de 9 de setembro de 2015.

serviço fornecido por transmissão de dados mediante pedido individual (art. 1.º, n.º 1, al. b*)*, iii*)* da Diretiva 2015/1535, de 9 de setembro de 2015), não se encontrando abrangidos, deste modo, os serviços fornecidos por envio de dados sem pedido individual e destinados à receção simultânea por um número ilimitado de destinatários (transmissão de «ponto para multiponto»)[133].

5. Conclusão

A definição de perfis é uma atividade empregada nos mais diversos planos da sociedade, consistindo num tratamento total ou parcialmente automatizado de dados pessoais com o propósito de avaliar certos aspetos pessoais de uma pessoa singular.

Embora o *profiling* seja um tratamento extremamente vantajoso, transportando utilidade e benefícios para as pessoas e organizações, não é uma atividade completamente inocente, encontrando-se a si associados sérios riscos e perigos cuja possível materialização acarreta ponderosos impactos negativos e injustificados nos direitos, liberdades e interesses dos titulares dos dados. Nesta senda, o Regulamento procura sujeitar diretamente a definição de perfis às regras nele próprio consagradas que regem o tratamento de dados pessoais, simultaneamente atribuindo ao titular poderes de reação suscetíveis de serem exercidos ainda que as operações efetuadas sobre dados pessoais sejam lícitas. Como tal, é conferido ao titular o direito de se opor ao *profiling*, cujo exercício, dentro dos pressupostos de aplicabilidade, impede o começo ou impõe a cessação do tratamento.

133 Anexo I da Diretiva 2015/1535, de 9 de setembro de 2015.

As *Smart Cities* e a Privacidade: o critério legal para a anonimização de dados agregados

JOANA DINIZ DE FIGUEIREDO[*]

Resumo: O presente estudo visa estudar a técnica de agregação de um ponto de vista legal de forma a determinarmos se os dados obtidos são anonimizados ou pessoais, e caso sejam pessoais, a partir de que momento é que deixam de ser. Esta conclusão é essencial para compreender se o tratamento de dados agregados no âmbito das Smart Cities encontra-se abrangido pelo RGPD1 . Para alcançar esta solução, analisámos o contexto das Smart Cities, o conceito de dados agregados e de anonimização, o modelo de agregação e concluímos através da definição de um critério que permite aferir o momento a partir do qual os dados agregados são dados anónimos à luz da lei aplicável.

***Palavras-chave**: cidades inteligentes; anonimização; dados agregados; privacidade; princípio do "privacy by design".*

Abstract: The aim of this study is to analyze the aggregation technique from a legal perspective to determine whether the obtained data is anonymized data or personal data. Moreover, it intends to ascertain, in this second case, when will it cease to be personal data. Such conclusion is essential to understand whether the processing of aggregated data within the scope of Smart Cities is covered by the GDPR. To achieve this solution, we analyzed the context of Smart Cities, the concept of aggregated data, and the concepts of technical

[*] Advogada e Consultora na área de Proteção de Dados, Direito Digital e TMT. Licenciada em Direito e Mestre em Direito Forense pela Universidade Católica Portuguesa, Faculdade de Lisboa.

and legal anonymization. Furthermore, we studied the aggregation model within the scope of Smart Cities and concluded by defining a criterion that allows us to determine when the aggregated data is anonymous according to the applicable law.

Keywords*: smart cities, anonymization, aggregated data, privacy, privacy by design.*

1. Introdução

O conceito de "Smart Cities" ou cidades inteligentes tem vindo a ganhar uma enorme importância nos últimos anos como um meio para fazer face aos desafios que a nossa sociedade enfrenta. A necessidade de aumentar a qualidade de vida dos cidadãos, a eficiência e a qualidade dos serviços, a adequação das medidas e serviços aos cidadãos e a sustentabilidade são alguns dos objetivos pretendidos nos dias de hoje e que despoletam os mais variados estudos e investigações.

Os projetos de Smart Cities têm como pedra de toque a utilização de novas tecnologias de informação que implicam a recolha de dados com grande precisão, qualidade e em grande quantidade. Tecnologias como a utilização de drones, impressoras 3D, Blockchain, Big Data, Internet of Things ("IoT"), Gamification, Smart Cars, Cloud e Inteligência Artificial ("IA") são consideradas o combustível das cidades inteligentes. Contudo, conforme analisaremos no presente estudo, esta recolha massiva de dados pessoais dos cidadãos poderá colocar variados desafios à privacidade e à proteção dos dados dos mesmos. Assim sendo, é necessária a procura de soluções que permitam que os municípios maximizem os benefícios desta recolha de dados com o total respeito pelos direitos, liberdades e garantias dos titulares dos dados.

Nesta senda, o presente estudo visa analisar uma solução que permita alcançar um equilíbrio entre a maximização da utilidade dos dados e o respeito pela proteção de dados dos cidadãos, em particular, através da técnica da agregação de dados. Ainda que muitas vezes seja considerado um método de anonimização de dados, vamos analisar se os dados resultantes da aplicação

desta técnica são dados pessoais ou se são dados anónimos para efeitos da legislação aplicável em matéria de proteção de dados.

A necessidade do presente estudo prendeu-se com a constatação da essencialidade do respeito pela privacidade dos cidadãos e da transparência relativamente aos projetos de Smart Cities. Apenas através de um projeto totalmente transparente podemos alcançar uma verdadeira proximidade com os cidadãos e a confiança dos mesmos. Contudo, estas considerações devem ser tomadas ad initium, alinhadas com os objetivos[1] do Regulamento Geral de Proteção de Dados (doravante designado por "RGPD" e "Regulamento")[2] e com o Princípio do Privacy by Design[3].

2. Smart Cities

2.1. Conceito

Como resultado do crescimento da população nas metrópoles, da redução dos recursos disponíveis e do desenvolvimento exponencial da tecnologia, as cidades têm vindo a ser estimuladas a encontrar novos métodos e soluções para alcançar uma maior eficiência, sustentabilidade, resiliência e incrementar a qualidade de vida dos cidadãos[4]. Através das cidades inteligentes (Smart Cities) procura-se responder a estes principais problemas enfrentados pelos espaços urbanos[5].

---

1 "(…) na proposta de Regulamento, a Comissão enuncia três grandes objetivos: 1- Permitir o desenvolvimento da economia digital; 2- Permitir que as pessoas singulares controlem os seus próprios dados; 3- Reforçar a segurança jurídica e prática para os operadores económicos e as entidades públicas." in Berberan Santos, Sofia e Gabriel, João, *Regulamento Geral Sobre a Proteção de Dados, Legislação e Algumas notas*, 3.ª Edição, Edição GPA Academy (2020), 20.

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.

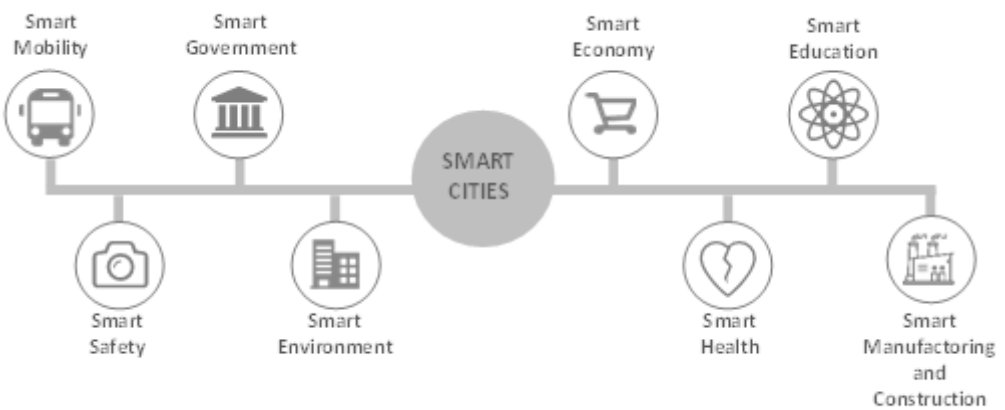
3 Cfr. art. 25.º do Regulamento Geral de Proteção de Dados.

4 "*Smart cities have emerged in this context as an answer to the growing problems of unsustainable urban expansion, growing inequality, climate change, and insecurity. Smart cities are urban centres that harness technologies such as big data, algorithms, and Internet of Things ('IoT') to enhance innovation and urban competitiveness.*" in Ranchordás, Sofia e Klop, Abram "Data-driven Regulation and Governance in Smart Cities", *Research Handbook in Data Science and Law*, 2 (2018).

5 "The vision of *''Smart Cities"* is the urban center of the future, made safe, secure

Assim sendo, as cidades consideram-se inteligentes quando o investimento em capital humano, infraestruturas tradicionais e tecnologias disruptivas estimulam o crescimento económico sustentável e a melhoria significativa da qualidade de vida, com uma gestão inteligente dos recursos naturais[6]. As cidades inteligentes são contruídas através de um conjunto de soluções ditas "inteligentes" nos diversos setores de atividade da nossa sociedade, onde são aplicadas tecnologias no sentido de incrementar a eficiência dos serviços e das tomadas de decisão (*vide* figura 1).

Figura 1 – Exemplos de Setores Abrangidos pelas Soluções Inteligentes



Fonte: Elaboração própria

A utilização das novas tecnologias para alcançar cidades sustentáveis, conectadas e otimizadas já não representa um futuro longínquo, sendo concebido como o meio principal para alcançar os objetivos referidos. Tecnologias como a utilização de drones, impressoras 3D, *Blockchain, Big Data, Internet of*

environmentally green, and efficient because all structures--whether for power, water, transportation, etc. are designed, constructed, and maintained making use of advanced, integrated materials, sensors, electronics, and networks which are interfaced with computerized systems comprised of databases, tracking, and decision-making algorithms." in Robert E. Hall/B. Boweman/J. Braverman/J. Taylor/H.Todosow/U.von Wimmersperg, The Vision of a Smart City, 2nd International Life Extension Technology Workshop, 1 (2000).

6 Deloitte, Smart Cities, How rapid advances in technology are reshaping our economy and society, version 1.0, (Nov.- 2015). Acessível em: <https://www2.deloitte.com/tr/en/pages/public-sector/articles/smart-cities.html> (consultado a 22 de novembro de 2020).

Things ("IoT"), Gamification, Smart Cars, Cloud e Inteligência Artificial ("IA") são consideradas o combustível das cidades inteligentes. Como foi apresentado por um relatório da Deloitte sobre *Smart Cities* "*[s]mart cities exist on the intersection of digital technology, disruptive innovation and urban environments. They are an exciting place to work and live and the breeding ground for new ideas*"[7]. As Tecnologias da Informação e Comunicação ("TIC") são desenvolvidas a uma velocidade sem precedentes ao longo dos últimos anos e a conjunção destas com os ambientes urbanos está a criar ambientes urbanos bastante diferentes do experimentado até agora.

Neste contexto, os projetos e programas de Smart Cities começam a emergir por todo o mundo como um novo paradigma e como a resposta adequada aos desafios da nossa sociedade.

A *PricewaterhouseCoopers* (doravante designada "PwC"), num estudo sobre *Smart Cities*[8], vem apresentar os seis desenvolvimentos tecnológicos e financeiros considerados críticos para impulsionar o crescimento das Smart Cities: i) as parcerias público-privadas; ii) o desenvolvimento de tecnologias emergentes (e.g., *blockchain, smart cars, IoT*); iii) a expansão da infraestrutura de TIC (e.g., evolução 4G, lançamento do 5G); iv) foco na cibersegurança (i.e., proteção da informações da cidade e dos dados dos cidadãos); v) *Cloud, edge and fog computing* (i.e., existe a necessidade de armazenamento em tempo real dos dados tendo em consideração o volume, a variedade e a velocidade dos mesmos); e vi) *Open data* e *Big Data Analytics*.

2.2. Os desafios para a privacidade

Os benefícios das *Smart Cities* são visíveis e fundamentais para ultrapassar os desafios dos tempos atuais, contudo, são inegáveis os desafios inerentes à implementação das mesmas. Para alcançarmos soluções inovadoras e inteligentes, onde conseguimos avaliar consumos e a qualidade da água, a qualidade do ar, a movimentação e tráfego na cidade, será necessária a recolha

7 Deloitte, Smart Cities, cit.

8 PricewaterhouseCoopers, Creating the Smart Cities of the future in Security and Privacy in your Smart City (Maio - 2019). Acessível em: <https://www.pwc.com/gx/en/sustainability/assets/creating-the-smart-cities-of-the-future.pdf> (consultado a 22 de novembro de 2020).

de grandes volumes e variedades de dados. A recolha massiva de dados e informações através de tecnologias de monitorização para a gestão das cidades inteligentes pode gerar insegurança para a privacidade dos cidadãos.

A recolha de dados através de tecnologias de *big data* e algoritmos e o respetivo tratamento dos mesmos são considerados o "coração" das *Smart Cities* ("*Data is the lifeblood of modern public policy*"[9]). Os dados recolhidos alimentam os estudos, as estatísticas, as análises e permitem o desenvolvimento de tecnologias inteligentes e adequadas a cada cidade consoante as suas especificidades. Contudo, o surgimento destas tecnologias vem acompanhado de vários desafios práticos e legais que devem ser devidamente estudados e acautelados.

De entre os riscos que podem advir para a privacidade dos cidadãos apontamos como merecedores de especial atenção os ciberataques, a gestão dos dados recolhidos, a não priorização da segurança e da privacidade no momento do desenvolvimento das novas tecnologias, ameaças físicas aos dispositivos, a falta de maturidade para os temas de privacidade e cibersegurança e ataques à integridade, confidencialidade e disponibilidade dos dados.

Se não forem tomadas medidas de forma a reduzir e mitigar riscos inerentes a ciberataques e ciberterrorismo, os dados podem ser comprometidos de tal forma de acarretem prejuízos incalculáveis[10].

Tendo em consideração os impactos e danos que podem advir de uma utilização indevida dos dados pessoais é necessário procurar um equilíbrio entre a privacidade dos cidadãos e a qualidade dos dados para efeitos das *Smart Cities*. Este equilíbrio pode ser alcançado através da implementação de várias medidas técnicas de organizativas adequadas para assegurar um nível de segurança adequado ao risco, como a pseudonimização e a anonimização (Cfr. Art. 32.º do RGPD).

Ainda que seja bastante visível o diminuto nível de maturidade da população relativamente ao tema da privacidade e da proteção de dados, a

9 Ranchordás, Klop, Data-driven Regulation, cit., 6.

10 Em 2017, a empresa dinamarquesa Maesk foi alvo do ataque cibernético mais devastador da história, o NotPetya, tendo o valor de dados totais sido estimado em $ 10 biliões. O NotPetya foi um malware que, através desta empresa, alcançou muitas outras empresas do mundo, tendo sido caracterizado como um ato de guerra. Sobre este tema consultar: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> (Andy Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History) .

regulação dos últimos anos nesta matéria permitiu o aumento do nível de awareness da população face a estes temas. Exemplo ilustrativo do aumento do conhecimento da população para estes temas, ocorreu em agosto de 2019 em Hong Kong, onde um conjunto de manifestantes, que procuravam lutar pela privacidade e pela proteção dos seus dados, derrubaram postes de luz "inteligentes" equipados de sensores e câmaras, por não se conformarem com a possível perda de privacidade[11].

2.3. A dicotomia entre os interesses públicos e privados

Os projetos de *Smart Cities*, como já referido anteriormente, assentam essencialmente na utilização de novas tecnologias para alcançar os seus objetivos, tecnologias estas que são providenciadas e desenvolvidas por empresas *Big Tech*. Estas empresas têm vindo a desenvolver soluções que permitem a mediação entre as cidades e os cidadãos e disponibilizam aos municípios não só os softwares, como também a implementação de sensores que recolhem dados dos cidadãos de forma massiva (*big data collection*) e que têm impacto na vida dos cidadãos.

Contudo, têm vindo a ser colocadas algumas questões relativamente aos interesses e valores destas empresas, em particular se estão ou não centrados nos cidadãos e nos valores e interesses públicos[12]. Estas questões têm vindo a ser levantadas por vários autores com fundamento na difícil conciliação entre os interesses e valores públicos e os interesses privados[13]. Isto porque as empresas *Big Tech* e as plataformas digitais estão imbuídas de valores privados centrados na maximização do lucro e no aumento da produtividade e eficiência que são substancialmente distintos dos valores e

11 Ranchordás, Sofia e Goanta, Catalina "The New City Regulators: Platform and Public Values in Smart and Sharing Cities", *University of Groningen Faculty of Law Research Paper Series*, No. 45/2019, (Out. - 2019).

12 Ranchordás e Goanta, The New City Regulators.

13 "While, for example, Huawei offers useful digital platforms for cities, it is also well-known that this company has been under investigation in different countries on suspicion of espionage and alleged trade-secret theft. This extreme example does not necessarily reflect the practices of other Big Tech companies, but it helps us illustrate the risks of a potential misalignment between public and private interests, the existence of hidden interests, and the lack of transparency of digital plat- forms." in Ranchordás, Goanta, The New City Regulators, cit.,8.

interesses públicos.

O potencial desequilíbrio entre os interesses públicos e privados levantam questões sobre a possível utilização indevida de dados pessoais de cidadãos e o desrespeito pela privacidade dos mesmos.

Os interesses e valores públicos que pretendem ser assegurados e alcançados com os projetos das *Smart Cities* são a qualidade de vida dos cidadãos e dos serviços públicos, a acessibilidade aos serviços públicos, a transparência, privacidade, a sustentabilidade e a igualdade do tratamento dos cidadãos.

No sentido de abordar este tema, Sofia Ranchordás e Catalina Goanta realizaram um estudo[14] onde procuraram compreender quais os potenciais conflitos de interesses e valores entre as empresas *Big Tech* e os interesses públicos e encontrar um equilíbrio entre os mesmos. Neste estudo foram apresentados alguns exemplos de potenciais interesses privados conflituantes, como é o caso da Huawei e do Airbnb. A Huawei, enquanto empresa que oferece soluções para cidades, foi alvo de investigações por suspeita de espionagem e roubo de segredos comerciais. Por outro lado, o Airbnb em Amesterdão causou uma crise imobiliária, colocando os direitos dos cidadãos e os valores públicos em causa. O caso do Airbnb é um exemplo de uma plataforma cujos interesses privados são conflituantes com interesses públicos, em particular refletido no enorme impacto causado nos moradores das cidades pelo aumento exponencial das casas em regime de alojamento local.

É inegável o desafio para estas empresas face à posição que assumem nestes projetos, na medida em que têm de se imbuir nos valores do bem público e gerar tecnologia dirigida para tal, afastando-se dos valores privados que lhes são inerentes. Contudo, ainda que os interesses possam ser distintos, tal não significa que os valores espelhados nas tecnologias e nos projetos desenvolvidos por empresas privadas não possam ser alinhados com os valores e interesses das empresas públicas.

Assim sendo, e na linha condutora do estudo elaborado por Sofia Ranchordás e Catalina Goanta[15], consideramos fundamental que no âmbito

14 Ranchordás e Goanta, The New City Regulators.
15 Ranchordás e Goanta, The New City Regulators.

dos projetos das Smart Cities sejam criadas normas legais que regulem esta colaboração de forma a garantir o acautelamento dos valores públicos e a boa-fé das empresas Big Tech nas negociações. A regulação desta relação tanto a nível legal como contratualmente é essencial para que se possa tirar proveito das tecnologias disponibilizadas pelas empresas garantindo que os valores públicos não são indevidamente prejudicados[16].

2.4. Privacy by design

O Regulamento Geral de Proteção de Dados, no seu art. 25.º, introduziu o princípio do *Privacy by Design*. Este princípio, desenvolvido na década de 90 pela Dra. Ann Cavoukian, procurou responder aos efeitos das tecnologias de informação e de comunicação na privacidade. O Princípio do *Privacy by Design* visa estabelecer de um padrão de atuação das organizações centrado na procura pela privacidade, que não é restringido ao mero cumprimento das normas legais existentes. O objetivo pretendido com a introdução deste princípio prende-se a antecipação da ponderação de todos os riscos que podem advir para os direitos, liberdades e garantias dos titulares dos dados, procurando mitigá-los à *priori*. Este princípio exige que as organizações incorporem a privacidade desde o design e a arquitetura dos projetos, sistemas ou práticas de negócio, tornando-se parte integrante dos mesmos.

O princípio do *Privacy by Design* é central no desenvolvimento dos projetos das *Smart Cities* tendo em consideração que consubstanciam projetos com recolha de grandes quantidades de dados pessoais, bem como através de tecnologias inovadoras, podendo implicar riscos para os direitos e liberdades dos titulares dos dados pessoais. O Princípio do *Privacy by Design*[17] implica

16 "In this context, we suggested a normative framework focusing on two points: departing from values shared by platforms and authorities, in order to shape a new kind of knowledge-service creation, namely local public-interest technology; and addressing the digital enforcement issue driven by the functional sovereignty role of platforms, by proposing a negotiated contractual system that seeks to balance platform values with public values." in Ranchordás e Goanta, The New City Regulators, cit., 32.

17 "*In essence, this means you have to integrate or 'bake in' data protection into your processing activities and business practices, from the design stage right through the lifecycle.*" in Information Commissioner's Office, Data protection by design and default. Acessível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-

uma ponderação *ad initium* das questões relativas à proteção de dados, de forma a avaliar e prevenir potenciais impactos das tecnologias necessárias ao desenvolvimento dos projetos das *Smart Cities* na privacidade dos cidadãos.

O cumprimento deste princípio deve ser garantido pelas entidades públicas que desenvolvam os projetos através da implementação de procedimentos internos e medidas técnicas e organizativas, bem como por todas as entidades subcontratadas para o desenvolvimento dos mesmos. O cumprimento por parte dos subcontratantes deve ser garantido através da celebração de um acordo em matéria de proteção de dados, onde devem ser estabelecidas exigentes medidas de segurança da informação, nos termos e para os efeitos dos art. 28.º e 32.º do Regulamento Geral de Proteção de Dados.

3. Agregação de dados

A agregação de dados é uma técnica utilizada comummente para fins estatísticos através da qual os dados são apresentados de forma resumida. Esta técnica é atualmente utilizada pela grande maioria dos setores de atividade, desde o setor do *marketing* ao setor da saúde, na medida em que permite a análise de grandes quantidades de dados obtendo informações resumidas e de consulta rápida e eficiente. A agregação de dados é uma técnica essencial para potenciar o crescimento dos negócios e monetizar os dados na medida em que permite às organizações a obtenção de dados fundamentais para a compreensão do negócio e das tendências de mercado.

No âmbito de projetos de *Smart Cities* a utilização desta técnica permite uma otimização dos dados recolhidos, reduzindo o risco de inconformidade com a legislação em vigor em matéria de proteção de dados e construindo e reforçando a confiança dos cidadãos nos projetos.

Através da técnica de agregação, os dados são recolhidos e são tratados posteriormente de forma a que sejam criados dados resumidos para análise. O processo de agregação contempla três fases: Recolha, Tratamento e Apresentação. Em primeiro lugar, existe uma recolha de dados pessoais (e.g., através de fontes de IoT) e são armazenados em bases de dados. De seguida, os dados recolhidos são agregados através de funções estatísticas e, por último, os

default/> (consultado a 22 de novembro de 2020)

dados são apresentados de forma agregada num formato resumido.

A técnica da agregação é incluída na maioria das vezes nas técnicas de anonimização de dados visto que poderá ter um efeito semelhante à técnica da anonimização quando os elementos individuais que permitam a identificação de uma pessoa singular sejam substituídos por dados referentes a grupos de pessoas. A utilização desta técnica reduz significativamente o risco para a privacidade dos titulares dos dados. No entanto, ao longo do presente estudo vamos analisar se, de um ponto de vista legal, os dados agregados são subsumíveis ou não no conceito de dados pessoais.

Esta técnica é utilizada quando não é necessário manter os dados com identificações pessoais e a utilização de dados agregados é suficiente para alcançar as finalidades pretendidas.

Nas tabelas abaixo exemplificamos o método de anonimização por agregação[18]. Na primeira tabela encontram-se os dados após a recolha e na segunda são apresentados os dados agregados. Neste exemplo objeto de anonimização foram recolhidos os códigos postais e consumos de água por ano numa amostra de oito consumidores.

Tabela 1 - Conjunto de dados após a recolha.

PESSOA	CÓDIGO POSTAL	CONSUMO DE ÁGUA (M^3/ HAB.) POR ANO
Pessoa A	1750-123	64,5
Pessoa B	1700-456	44,9
Pessoa C	1700-654	48,7
Pessoa D	1750-231	70,5
Pessoa E	1070-111	38,9
Pessoa F	1070-232	41,2
Pessoa G	1570-400	81,3
Pessoa H	1570-223	78.9

Fonte: Elaboração própria

18 Os dados apresentados são fictícios, servindo apenas para a finalidade de compreensão da técnica de anonimização.

Tabela 2 - Conjunto de dados agregados.

CÓDIGO POSTAL	INTERVALO DE CONSUMO DE ÁGUA (M^3/HAB.) POR ANO
1750	64,5 - 70,5
1700	44,9 - 48,7
1070	38,9 - 41,2
1570	78,9 - 81,3

Fonte: Elaboração própria

No exemplo apresentado nas tabelas 1 e 2 foi utilizada uma amostra de 8 consumidores, o que aumenta em larga medida o risco de re-identificação dos titulares dos dados. Contudo, não deixa de ser importante notar que esta técnica reduz significativamente a utilidade e a qualidade dos dados, não podendo ser utilizado em todas as situações, sob pena dos dados deixarem de ser úteis.

4. Anonimização de Dados Pessoais

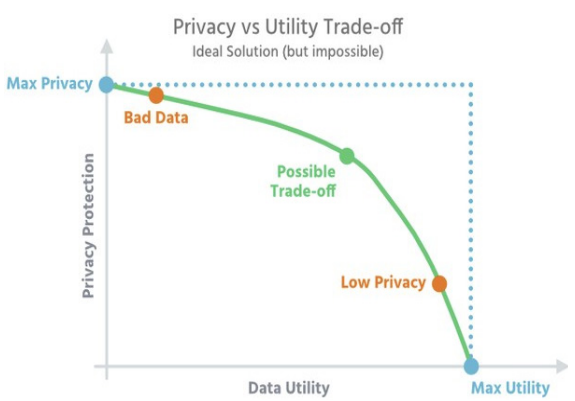
A técnica da anonimização surge nos últimos anos como uma ferramenta essencial para preservar a privacidade de conjuntos de dados que têm bastante valor e utilidade para as organizações. De forma a proteger a privacidade dos titulares dos dados, sempre que as organizações consigam manter a utilidade dos dados necessária para as finalidades estabelecidas, devem optar por esta técnica. Através da técnica da anonimização pretende-se balançar a utilidade dos dados pessoais e a privacidade dos mesmos de forma a que seja possível a transmissão de dados com redução da probabilidade de os mesmos serem associados a uma pessoa singular[19].

19 Parte da doutrina considera que este equilíbrio entre a utilidade dos dados e a anonimização é impossível de alcançar. Nas palavras de Paul Ohm "(…) research unearths a tension that shakes a foundational belief about data privacy: Data can be either useful or

A anonimização ideal é obtida através da maximização da privacidade e da utilidade dos dados (*trade-off*), o que é bastante difícil de alcançar, tendo em consideração que todos os modelos de anonimização utilizados padecem de limitações e que, na maioria dos casos, existe uma necessidade de interligação de registos entre bases de dados distintas.

O gráfico abaixo pretende facilitar a compreensão da relação entre a privacidade e a utilidade dos dados pessoais, sendo possível concluir que, à medida que ganhamos privacidade relativamente a um conjunto de dados pessoais, a utilidade dos mesmos diminuí. A diminuição da privacidade consubstancia-se essencialmente na possibilidade de terceiros re-identificarem pessoas singulares. O aumento da utilidade dos dados ocorre quando se aumenta a quantidade de informações sobre os indivíduos, obtendo informações mais completas[20].

Figura 2 - Privacidade vs. Utilidade dos dados pessoais



Fonte: SARTOR, Nicolas. Data Anonymisation Software – Differences Between Static and Interactive Anonymisation. Disponível em: <https://www.datasciencecentral.com/profiles/blogs/data-anonymisation-software-differences-between-static-and>

No entanto, é fundamental ter em consideração que a figura é meramente ilustrativa e que a comparação destas duas variáveis (i.e., utilidade

perfectly anonymous but never both." In Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, *57 UCLA Law Review* 1701 (2010), cit., 1704.

20 Tiancheng Li, Ninghui Li, On the Tradeoff Between Privacy and Utility in *Data Publishing*, Department of Computer Science Purdue University (2009).

e privacidade dos dados) não representa na realidade um ganho e uma perda proporcionais, variando de acordo com vários fatores incluindo a utilização de dados individuais ou dados agregados[21].

4.1. Anonimização e pseudonimização

A anonimização e a pseudonimização (ou utilização de pseudónimos) são suas técnicas que, embora sejam muitas vezes confundidas, representam duas realidades distintas e com diferentes impactos para a proteção de dados.

O processo de anonimização permite a conversão irreversível de dados pessoais em dados não identificáveis. Por sua vez, a pseudonimização é definida nos termos do n.º 5 do art. 4.º, do Regulamento Geral de Proteção de Dados como um *"(...) [t]ratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável*". A pseudonimização permite que o Responsável pelo Tratamento[22] associe os dados aos titulares dos dados pessoais através de um processo em que se substituí todos os identificadores pessoais por pseudónimos, que podem ser códigos gerados artificialmente para mascarar os dados originais.

A grande distinção entre ambos consiste no carácter definitivo da anonimização e na possibilidade de reversibilidade da pseudonimização. Consequentemente, a legislação em matéria de proteção de dados é aplicável à pseudonimização, na medida em que permite a identificação dos titulares dos dados, ainda que indiretamente. Ao invés, a anonimização, constituindo um tratamento irreversível, é excluída do âmbito de aplicação da legislação relativa à proteção de dados.

Contudo, cumpre notar que a pseudonimização não deixa ter uma enorme importância enquanto medida técnica, nos termos do art. 32.º do RGPD,

21 Tiancheng Li e Ninghui Li, *On the Tradeoff*.

22 O conceito de Responsável pelo Tratamento deve ser entendido nos termos e para os efeitos do n.º 7 do art.4.ºdo Regulamento Geral de Proteção de Dados.

para efeitos de segurança de informação. A utilização desta técnica reduz a capacidade de ligação de um conjunto de dados à identidade dos seus titulares e, para obtenção de uma pseudonimização com um caráter mais "forte", são utilizados mecanismos de atribuição de códigos aleatórios.

4.2. Anonimização técnica

A anonimização é uma técnica através da qual se pretende obter a conversão de dados identificáveis em dados não identificáveis.

A anonimização encontra-se definida em normas internacionais, como é o caso da ISO 29100:2011[23] onde é defina como "*process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party*".

O processo de anonimização visa tornar os dados anónimos, no entanto existem diversas técnicas que podem ser utilizadas para o efeito. Estas técnicas, ainda que com o mesmo objetivo, apresentam níveis de re-identificação distintos variando de acordo com o *data set* utilizado.

As diferentes técnicas de anonimização devem ser utilizadas consoante a situação em causa, na medida em que técnica tem especificidades que podem ser benéficas para diferentes tipos de situações.

Existem duas abordagens distintas para alcançar a anonimização dos dados pessoais, em particular, a Aleatorização e a Generalização, que passamos abaixo a detalhar.

4.2.1. Aleatorização (Randomization)

A técnica da Aleatorização (*Randomization*) visa a alteração da veracidade dos dados pessoais de forma que não seja possível a ligação dos dados às pessoas em causa. Esta técnica baseia-se na introdução de um fator de incerteza nos dados, contribuindo para a diminuição da associação entre os dados e as pessoas singulares.

23 ISO/IEC 29100:2011, Information technology — Security techniques — Privacy framework

As principais técnicas de anonimização por aleatorização são a introdução de ruído (*Noise Addition*), a permutação (*Shuffling*) e a privacidade diferencial (*Differential Privacy*). Para garantir a total irreversibilidade dos dados, podem ser utilizadas várias técnicas em simultâneo.

A técnica da introdução de ruído é uma das técnicas mais utilizada e consiste na introdução de ruído nos dados de forma a conferir confidencialidade aos mesmos. Contudo, tem-se vindo a constatar que com a tentativa de alcançar uma maior confidencialidade dos dados e um menor risco de re-indetificação, esta técnica tem vindo a perder algumas propriedades estatísticas.

4.2.2. Generalização

A generalização é uma técnica de anonimização de dados que consiste em generalizar ou diluir os dados pessoais através da alteração da escala ou ordem de grandeza[24].

As principais técnicas de anonimização por generalização são a agregação[25] e kanonimato e a L-diversidade/t-proximidade.

Uma das técnicas mais utilizadas, e com maior importância para o estudo em causa, é a técnica da agregação. As técnicas de agregação e k-anonimato "(…) visam impedir que um titular dos dados seja selecionado através do agrupamento com, pelo menos, outras k pessoas"[26]. Esta técnica permite que os titulares dos dados não sejam identificados na medida em que os dados pessoais são partilhados por vários utilizadores (k utilizadores). Os dados são generalizados de forma a que vários titulares partilhem dos mesmos dados.

5. Anonimização Legal

24 GT 29, Parecer 05/2014 do Grupo de trabalho do artigo 29.º sobre técnicas de anonimização, adotado em 10 abril de 2014.

25 A técnica da agregação encontra-se desenvolvida no capítulo "D. Agregação de Dados".

26 GT 29, Parecer 05/2014.

Como já foi referido anteriormente, a anonimização é uma técnica que é aplicada a dados pessoais com o objetivo de evitar de forma irreversível a identificação do titular dos dados e é antecedida de um processo de recolha de dados que carece do cumprimento da legislação em vigor em matéria de proteção de dados pessoais.

O Regulamento Geral de Proteção de Dados entre os princípios relativos ao tratamento de dados pessoais, estabelece o princípio da limitação das finalidades, nos termos da alínea b) do n.º 1 do art. 5.º, nos termos do qual os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de forma incompatível com essas finalidades. Este princípio consagra ainda que não é considerado incompatível com as finalidades iniciais, o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos.

Ora, através da técnica da anonimização é possível a utilização dos dados para finalidades distintas, sem a limitação que nos é exigida pelo princípio da limitação das finalidades.

A Diretiva 95/46/CE, no seu considerando 26, excluía do seu âmbito de aplicação os dados objeto de anonimização, referindo expressamente que *"(...) os princípios da protecção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável (...)*".

Com a entrada em vigor do Regulamento Geral de Proteção de Dados que veio revogar a Diretiva 95/46/CE, o legislador manteve a exclusão da aplicação da legislação relativa a proteção de dados pessoais aos dados anonimizados. Nos termos do considerando 26 do mesmo, é estabelecido que *"(...) [o]s princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação*".

O considerando 26 do RGPD oferece-nos uma definição de anonimização detalhando que os dados pessoais são considerados anónimos

quando não dizem respeito a uma pessoa identificada ou identificável. Ora, consequentemente, quando uma informação "diz respeito a uma pessoa singular identificada ou identificável", esta informação é qualificável como "dado pessoal" nos termos e para os efeitos da alínea a) do n.º 1 do art. 4.º do RGPD. Assim sendo, parece claro que para determinarmos se um conjunto de dados se encontra anonimizado é necessário avaliar se a informação permite identificar ou torna identificável os titulares dos dados.

Adicionalmente, o considerando 26 do RGPD avança ainda um critério para determinar se uma pessoa singular é ou não identificável. O critério escolhido pelo legislador para aferição da identificabilidade de pessoas singulares foi o critério da razoabilidade. Assim sendo, deverão ser tomados em consideração "(…) todos os meios suscetíveis de ser razoavelmente utilizados (…)".

Para o entendimento cabal do conceito que nos é oferecido pelo Regulamento Geral de Proteção de Dados de anonimização é crucial compreendermos o significado de dado pessoal e dos elementos que o compõem, nos termos do n.º 1 do art. 4.º do mesmo.

5.1. Definição de dados pessoais

O estudo do conceito de Dados Pessoais é fundamental para compreendermos o conceito de anonimização.

O conceito de dados pessoais consta do n.º 1 do art. 4.º do RGPD consubstanciando-se em toda a "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)". O referido art. acrescenta ainda que *"(...) é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular*".

A definição de dados pessoais que nos é concedida pelo Regulamento Geral de Proteção de Dados é composta essencialmente por 5 elementos, em particular: i) informação; ii) relativa a; iii) uma pessoa singular; iv) identificada;

e v) identificável.

Para um total entendimento do conceito de dados pessoais é necessária a compreensão detalhada dos elementos que o constituem.

a) Informação

A expressão "informação" denota a intenção do legislador em criar um conceito amplo de dados pessoais. O Grupo de Trabalho do Artigo 29[27], relativamente a este conceito, incluí todas as informações objetivas ou factuais (e.g., determinado parâmetro num exame médico, nacionalidade de uma pessoa) e as informações subjetivas (e.g., opiniões, avaliações, testes psicotécnicos) sobre determinada pessoa.

A informação tem relevância para o Direito da Proteção de Dados independentemente do suporte ou formato em que for recolhida e armazenada, incluindo o formato alfabético, fotográfico, numérico, gráfico, suporte papel, código binário, CD ou cassete[28].

Por outro lado, não com menor relevância, têm-se vindo a discutir se a informação no contexto do n.º 1 do art. 4º, tem de ser verdadeira. Alguns autores têm vindo a defender que a informação não necessita de ser verdadeira ou comprovada, com base no argumento de que o próprio Regulamento Geral de Proteção de Dados, no seu art. 16.º, confere ao titular dos dados o direito de solicitar a retificação dos dados que considere inexatos. Ora, o próprio RGPD parte do pressuposto que os dados podem não se encontrar exatos e verdadeiros, conferindo o direito à retificação, não excluindo tais dados do seu âmbito de aplicação.

No que concerne ao conteúdo da informação, o conceito de dados pessoais abrange os mais variados aspetos relativamente ao titular dos dados pessoais, nomeadamente físicos, mentais, familiares ou sociais. As informações sobre os titulares incluem dados identificativos (e.g., nome, número de identificação, data de nascimento), dados de localização, características físicas (e.g., peso, altura, cor da pele, cabelo, olhos) e identificadores por via eletrónica (Cfr. art.

27 GT 29, Parecer 4/2007 do Grupo de trabalho do art. 29.º sobre o conceito de dados pessoais, adotado em 20 de junho.

28 *Ibidem*.

4º, n.º 1 do RGPD). O conceito de informação abrange ainda todos os dados que revelem a origem racial ou étnica, opiniões políticas ou filosóficas, filiação sindical, dados genéticos, dados biométricos que identifiquem uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual (Cfr. art. 9.º do RGPD).

b) Relativa a

A expressão "relativa a" vem restringir a informação à pessoa a que respeita. Para que a informação seja considerada um dado pessoal tem de estar relacionada com uma pessoa, tem de ser informação sobre uma pessoa.

Nas palavras de A. Barreto Menezes Cordeiro *"[e]sta intrínseca relação entre a informação e um sujeito excluí o campo de aplicação do RGPD toda a informação concernente a realidades jurídicas não subjetiváveis*".

Algumas informações são facilmente associadas a pessoas singulares, contudo existem informações que apresentam uma maior dificuldade na determinação da relação com pessoas singulares. Quando as informações são referentes a objetos ou constituem dados factuais é necessária uma avaliação casuística para a determinação de uma possível relação com uma pessoa singular. Um exemplo elucidativo que nos é apresentado pelo Grupo de Trabalho do Artigo 29.º relativamente ao conceito de dados pessoais prende-se com o registo de um carro numa oficina que contempla variadas informações sobre o carro (e.g., os quilómetros, as revisões, as condições do material). O Grupo de Trabalho do Artigo 29.º vem-nos dizer que, analisados os dados individualmente, poderiam não constituir dados pessoais, contudo, relacionado com o proprietário para efeitos de faturação, constitui informação "relativa ao" proprietário[29].

O Grupo de Trabalho do Artigo 29.º, a este respeito, vem sintetizar três elementos alternativos que permitem considerar uma informação "relativa a" uma determinada pessoa: os elementos de conteúdo, de finalidade e de resultado[30]. O elemento de conteúdo representa toda a informação sobre uma pessoa singular (e.g., os exames médicos que são realizados a um doente,

29 GT 29, Parecer 4/2007.
30 *Ibidem*.

logo essa informação respeita ao doente). No elemento da finalidade, os dados utilizados têm como finalidade "avaliar, tratar de determinada forma ou influenciar o estatuto ou comportamento de uma pessoa"[31]. No que respeita ao elemento de resultado, estão em causa todas as informações que são relativas a uma pessoa porque o tratamento das mesmas pode ter impactos nos direitos e interesses da pessoa em causa.

c) Uma pessoa singular

O Regulamento Geral de Proteção de Dados restringe a aplicação dos princípios de proteção de dados a informações relativas a pessoas singulares independentemente da sua nacionalidade ou do seu local de residência (Cfr. Considerandos 14 e 26 do RGPD). No considerando 14 do RGPD é excluída a proteção conferida pelo mesmo a pessoas coletivas ficando ainda de fora "*(...) demais realidades jurídicas não subjetiváveis, como coisas e os animais*"[32].

No que concerne à exclusão dos objetos cumpre alertar que poderão existir informações relativas a objetos que possam constituir dados pessoais de determinada pessoa singular. Pegando novamente no exemplo do registo de um veículo numa oficina, onde constam as informações sobre o veículo, é evidente que as informações relativas ao veículo em si não constituem dados pessoais, no entanto, se relacionadas com uma pessoa singular podem constituir dados pessoais.

Ainda que a legislação em matéria de proteção de dados exclua do seu âmbito de aplicação a proteção de pessoas coletivas, importa ter em consideração que, em determinados casos, poderá ser aplicável a informações relativas a empresas e/ou pessoas coletivas. Quando a informação relativa a empresas e/ou pessoas coletivas também seja relativa a pessoas singulares (quando verificado um dos elementos de "conteúdo", "finalidade" ou "resultado"), também deverá ser qualificada como dado pessoal e consequentemente devem ser aplicadas as regras relativas à proteção de dados.

O considerando 27 do RGPD esclarece ainda que o Regulamento "(…)

31 GT 29, Parecer 4/2007.

32 Cordeiro, A. Barreto Menezes, Dados pessoais: conceito, extensão e limites, Revista de Direito e Tecnologia, Vol.1 (2019), n.º 2 (2018), p. 297-321, 10. Acessível em: <https://blook.pt/publications/fulltext/e38a9928dbce/>

não se aplica aos dados pessoais de pessoas falecidas". No entanto, a Lei n.º 58/2019, de 8 de agosto, que assegura a execução do Regulamento Geral de Proteção de Dados, no ordenamento jurídico português, no seu art. 17.º, vem alargar o âmbito de aplicação do RGPD, protegendo ainda os dados de pessoais de pessoas falecidas quando se tratem de categorias especiais de dados pessoais (art. 9.º do RGPD), quando se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações. Os direitos consagrados no Regulamento Geral de Proteção de Dados podem ser exercidos por quem tenha sido designado para o efeito pela pessoa falecida ou, na sua falta, pelos seus herdeiros (Cfr. art. 17.º, n.º 2 do RGPD). No entanto, se os dados disserem respeita ao falecido e a outro titular vivo, a informação deixa de poder ser livremente utilizada.

d) Conceito de pessoa identificada

O Regulamento Geral de Proteção de Dados define dados pessoais como a informação relativa a uma pessoa singular identificada ou identificável (Cfr. art. 4.º, n.º 1 do RGPD). O Regulamento, acrescenta ainda que "é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

O legislador utilizou a expressão "direta" para caracterizar as situações em que uma pessoa singular é identificada sem necessidade de recorrer de recorrer a dados adicionais. O Tribunal de Justiça da União Europeia, no Acórdão Breyer, vem esclarecer relativamente ao tema dos IPs dinâmicos dos utilizadores que "(…) deve-se, antes de mais, salientar que é dado assente que um endereço IP dinâmico não constitui uma informação relativa a uma «pessoa singular identificada», na medida em que esse endereço não revela diretamente a identidade da pessoa singular proprietária do computador a partir do qual se efetua a consulta de um sítio Internet, nem a de outra pessoa que possa utilizar esse computador".

Schwartz, a este respeito, vem referir que "*[a]mong EU member states that have traditionally taken a leading role in information privacy law, a person falls in the "identified" category if a party can use information relating to her to determine her specific identity*"[33].

Uma pessoa considera-se identificada quando a informação em causa respeita diretamente a essa pessoa e seja suficiente para a identificar inequivocamente, sem que sejam necessárias informações adicionais[34]. Exemplos de dados que respeitam a uma pessoa singular identificada são o nome completo de uma pessoa, o cartão de cidadão, a sua impressão digital, o NIF.

e) Conceito de pessoa identificável

O conceito de pessoa identificável é um conceito-chave para a verdadeira compreensão do significado de dados pessoais e de anonimização. Contudo, este conceito é complexo e tem vindo a ser objeto de diversas e distintas interpretações.

Para que uma pessoa seja considerada identificável é necessário que seja possível identificar o titular dos dados com informações adicionais sobre o mesmo. Ou seja, ainda que determinado dado não permita identificar o titular dos dados, conjugada com outra informação é possível a identificação do titular.

Nos termos do considerado 26, o Regulamento refere ainda que, "*[p]ara determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica*"[35].

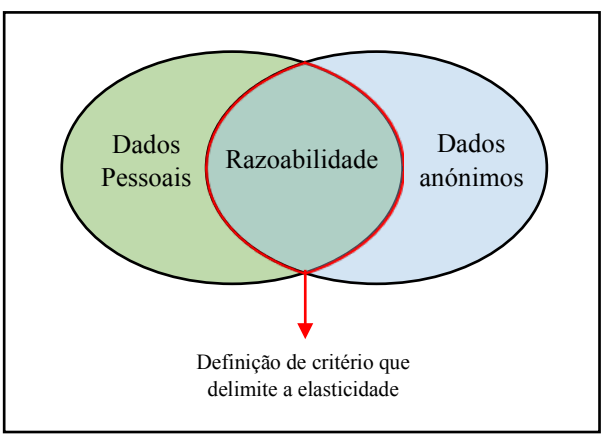
33 Schwartz, Paul M. e Solove, Daniel J., Reconciling Personal Information in the United States and European Union, Vol. 102:877, *California Law Review,* (2014), cit., 882.

34 Cordeiro, A. Barreto Menezes, Dados pessoais, cit., 14 ss.

35 TJUE 19-out.-2016, proc. C-582/14 (Acórdão Breyer).

O Regulamento Geral de Proteção de Dados apresenta-nos um conceito amplo e indeterminado de dados pessoais o que torna mais complexa a distinção entre dados pessoais e dados anonimizados. Assim sendo, implica a necessidade de definição de um critério que permita a distinção entre dados pessoais e dados anonimizados sob pena da fronteira entre ambos ser transponível. Este critério deverá delimitar da elasticidade do conceito de dados pessoais, em particular o termo identificável.

Figura 3 – Dados Pessoais vs Dados Anónimos



Fonte: Elaboração própria

O Regulamento Geral de Proteção de Dados apresenta-nos como critério para aferição do conceito de "identificável" o critério da razoabilidade. A interpretação do conceito de "identificável" será interpretado casuisticamente pelo intérprete, consoante os dados em causa e com os meios suscetíveis de serem razoavelmente utilizados para identificar direta ou indiretamente a pessoa singular. Nas palavras de A. Barreto Menezes Cordeiro *"[a] assunção de um critério de razoabilidade é um reflexo da impossibilidade fáctica de garantir a anonimidade absoluta dos dados recolhidos*".

O critério da razoabilidade que nos é oferecido pelo RGPD visa limitar a elasticidade do conceito de dados pessoais restringindo a qualificação do conceito de dados pessoais a um esforço razoável em obtê-los. Este critério

deve ser interpretado de acordo com dois tipos de fatores: i) fatores objetivos; e ii) fatores subjetivos. Os fatores objetivos, encontram-se elencados no considerando 26 do RGPD e consistem nos seguintes: custos, tempo necessário para a identificação, a tecnologia disponível à data do tratamento de dados e a evolução tecnológica. Estes fatores implicam uma análise dinâmica e que varia consoante o momento do tratamento de dados pessoais. Os fatores subjetivos apresentados pelo legislador relativamente ao critério da razoabilidade prendem-se com os meios suscetíveis de serem razoavelmente utilizados pelo responsável pelo tratamento ou por outra pessoa. Estes fatores respeitam à capacidade individual de engenharia reversa de quem procede ao tratamento dos respetivos dados pessoais.

O legislador procurou apresentar um critério tecnologicamente neutro, não apontando diretamente para nenhuma tecnologia concreta[36]. O objetivo desta escolha foi o desenho de uma norma que permite o acompanhamento constante do desenvolvimento tecnológico, tendo em consideração que ao longo deste desenvolvimento surgirão cada vez mais tecnologias que tornarão mais provável a re-identificação de dados anonimizados. Assim sendo, o conceito de dados pessoais deve também ser avaliado no momento concreto em que se pretende efetuar um tratamento de forma a ser ponderado o estado tecnológico do momento.

No que respeita aos meios suscetíveis de serem razoavelmente utilizados pelo responsável pelo tratamento ou por outra pessoa existem dois problemas que são apresentados pela doutrina e jurisprudência: i) a possibilidade de serem utilizados meios ilícitos para a identificação do titular dos dados; ii) a relevância da informação obtida através de meios suscetíveis de serem razoavelmente utilizados por outras pessoas.

No que concerne à licitude dos meios, o Tribunal de Justiça da União Europeia (doravante designado "TJUE"), no Acórdão Breyer o advogado-geral considerou que *"(...) assim não será se a identificação da pessoa em causa for proibida por lei ou inexequível, por exemplo devido ao facto de implicar um esforço desmedido em termos de tempo, de custo e de mão de obra, de*

36 "*A fim de se evitar o sério risco sério de ser contornada a proteção das pessoas singulares, esta deverá ser neutra em termos tecnológicos e deverá ser independente das técnicas utilizadas*", considerando 15 do RGPD.

modo que o risco de uma identificação parece na realidade insignificante"[37]. Em suma, o presente acórdão vem considerar que as informações obtidas por meios ilícitos não devem ser tomados em consideração para efeitos do conceito de "identificável" sob pena de implicar um esforço desmedido.

Contudo, a posição do TJUE tem vindo a ser bastante criticada pela doutrina. Os argumentos apresentados pela doutrina em sentido contrário ao acórdão Breyer centramse essencialmente nas diferenças legislativas que existem nos vários ordenamentos jurídicos podendo em determinados países ser considerado um meio lícito e noutros ilícito, bem como a frequência da ocorrência de ataques informáticos[38]. Nesta sequência, A. Barreto Menezes Cordeiro afirma que "*(...) sendo o critério último o da razoabilidade, importa atender a todas as condutas ilícitas que possam razoavelmente contar com elas*"[39]. O autor baseia a sua afirmação em três elementos interpretativos, o elemento literal, através do qual refere que o critério de razoabilidade apresentado no considerando 26 não excluí ilicitudes, o elemento teleológico onde é realçado o objetivo do Regulamento Geral de Proteção de Dados em defender a devassa da vida privada no seu todo, e o elemento sistemático que permite a conclusão de que o direito da proteção de dados foi criado tendo em consideração que os dados dos titulares podem ser obtidos ilicitamente[40].

No que respeita à segunda problemática abordada e debatida pela doutrina é discutida a relevância da informação obtida através de meios suscetíveis de serem razoavelmente utilizados por outras pessoas. Quanto a esta problemática a doutrina tem vindo a dividir-se essencialmente, ainda que com algumas variações, em duas teorias: a teoria relativa e a teoria absoluta.

Por um lado, a teoria relativa vem considerar que para a determinação do conceito de "pessoa singular identificável" devem ser apenas tidos em consideração os meios e conhecimentos detidos pelo Responsável pelo Tratamento. Por outro lado, os defensores a teoria absoluta consideram que devem não só ser tomados em consideração os meios e conhecimentos detidos

37 TJUE 19-out.-2016, proc. C-582/14 (Acórdão Breyer).

38 Cordeiro, A. Barreto Menezes, Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2018, Almedina, Coimbra (2020) 123.

39 Cordeiro, A. Barreto Menezes, Direito da Proteção, 123.

40 *Ibidem*.

pelo Responsável pelo Tratamento como por terceiros.

A teoria relativa é defendida pela maioria da doutrina e jurisprudência alemã[41]. Um dos principais argumentos dos defensores da teoria relativa prende-se com a impossibilidade de um anonimato absoluto e irreversível. Neste sentido, Paul Ohm conclui que "*Computer scientists have recently undermined our faith in the privacy protecting power of anonymization, (...). These scientists have demonstrated that they can often "reidentify" or "deanonymize" individuals hidden in anonymized data with astonishing ease. By understanding this research, we realize we have made a mistake, labored beneath a fundamental misunderstanding, which has assured us much less privacy than we have assumed. This mistake pervades nearly every information privacy law, regulation, and debate, yet regulators and legal scholars have paid it scant attention*".

O Regulamento Geral de Proteção de Dados, no considerando 4, reconhece que o direito à proteção de dados não é absoluto e enaltece a dimensão económica do tratamento de dados pessoais. O direito à proteção de dados, não constitui um direito absoluto, e deve ser analisado de acordo com a sua função na sociedade e ser equilibrado com outros direitos fundamentais. Adicionalmente, a Comissão Europeia elencou como um dos grandes objetivos do Regulamento Geral de Proteção de Dados, para além da devolução do controlo aos titulares dos dados, o desenvolvimento da economia digital.

O enaltecimento da dimensão económica do tratamento dos dados pessoais é outro argumento central e fundamental para a compreensão da teoria relativa. O alargamento excessivo do conceito de dados pessoais vai pôr em causa a dimensão económica do tratamento dos dados e os interesses económicos da União Europeia e dos seus estados-membros face ao processo de globalização, limitando as possibilidades de utilização dos mesmos.

Adicionalmente, caso aplicássemos a teoria objetiva pura, todos os dados seriam considerados dados pessoais, na medida em dificilmente se alcança a inexistência de risco de re-identificação, o que, inevitavelmente, vai ter impacto tanto na dimensão económica do direito.

41 Cordeiro, A. Barreto Menezes, Direito da Proteção, 127.

Por outro lado, a doutrina defensora da teoria relativa argumenta ainda que:

i) A atribuição da relevância aos meios e conhecimentos detidos por terceiros impossibilitaria que o Responsável pelo Tratamento conhecesse se está ou não a respeitar a legalidade, tendo em consideração que esta poderá respeitar a um responsável sediado noutro país;

ii) Tornaria o processo de supervisão por parte das entidades responsáveis excessivamente pesado ou praticamente impossível;

iii) Consubstanciaria uma colisão de interesses, entre os interesses pessoais (i.e., proteção dos seus dados pessoais) e os interesses coletivos (i.e., livre iniciativa económica);

iv) Colocaria em causa a possibilidade de realização de estudos estatísticos.

No considerando 26 do RGPD o legislador faz referência a "*(...) todos os meios suscetíveis de ser razoavelmente utilizados, (...) quer pelo responsável pelo tratamento quer por outra pessoa*". Neste considerando é visível a referência do legislador face aos meios utilizados por terceiros. No entanto, de acordo com os defensores da teoria relativa esta expressão não conduz a uma teoria absoluta, na medida em que não se refere a todos os meios disponíveis por terceiros, mas apenas aqueles que possam ser razoavelmente utilizados. E os meios que podem ser razoavelmente utilizados por terceiros também devem ser levados em consideração pelo Responsável pelo Tratamento no âmbito da teoria relativa.

Face aos argumentos apresentados pela doutrina defensora da teoria relativa, os defensores da teoria objetiva consideram que sendo o critério aplicável o da razoabilidade, esta teoria nunca poderia ser objetiva na aceção pura no termo[42].

O Tribunal de Justiça da União Europeia, no acórdão Breyer, pronunciou-se acerca desta questão considerando que *"(...) um endereço IP dinâmico registado por um prestador de serviços de meios de comunicação em linha aquando da consulta por uma pessoa de um sítio Internet que esse prestador disponibiliza ao público constitui, relativamente a esse prestador,*

42 Cordeiro, A. Barreto Menezes, Direito da Proteção, 128.

um dado pessoal na aceção dessa disposição, quando este disponha de meios legais que lhe permitam identificar a pessoa em causa graças às informações suplementares que o fornecedor de acesso à Internet dessa pessoa dispõe"[43]. Face à presente decisão do TJUE, A. Barreto Menezes Cordeiro vem referir que *"[a] posição sufragada pelo TJUE não é fácil de catalogar, na medida em que rejeita a teoria relativa, mas, ao mesmo tempo, rejeita a teoria objetiva no seu estado mais puro*"[44].

6. Utilização dos dados agregados no âmbito dos projetos de Smart Cities

6.1. Contexto

Este estudo é centrado na privacidade dos dados da comunidade na medida em que consideramos que os pilares essenciais da arquitetura de uma cidade inteligente são a transparência, confiança dos cidadãos e respeito pela privacidade dos mesmos. Apenas através da criação de um projeto totalmente transparente perante os cidadãos se consegue alcançar o sucesso do projeto. Por outro lado, é fundamental que desde a origem do projeto seja proactivamente tomada em consideração a privacidade e sejam desenhadas medidas técnicas e organizativas para garantir o total respeito pela legislação em matéria de proteção de dados, bem como prevenir e antecipar riscos (Princípio do *Privacy by Design*). O reconhecimento do valor e dos benefícios da adoção de medidas fortes ao nível da privacidade é essencial para garantir o respeito pelos direitos, liberdades e garantias dos titulares dos dados.

Através do presente estudo, pretendemos debruçar-nos sobre uma solução que por um lado garanta o respeito pelos direitos fundamentais dos cidadãos, em particular, o direito à privacidade e, por outro, permita a utilização dos dados dos mesmos para efeitos de desenvolvimento de cidades inteligentes. No que respeita ao desenvolvimento das cidades inteligentes, vamos centrar o nosso estudo no aproveitamento e otimização dos dados que já foram recolhidos para determinadas finalidades de forma a ser possível a utilização para outras finalidades, que não careçam da identificação dos titulares dos dados. Estas

43 TJUE 19-out.-2016, proc. C-582/14 (Acórdão Breyer).

44 Cordeiro, A. Barreto Menezes, Direito da Proteção, 129.

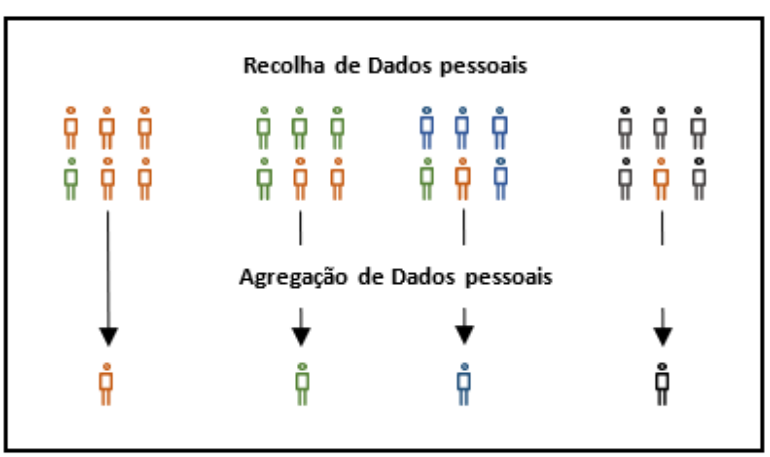
finalidades, no âmbito dos projetos das *Smart Cities*, são a caracterização da população e a compreensão das tendências para a prestação de um melhor serviço público. Analisadas as características e tendências dos munícipes, é possível a adequação de medidas, políticas, serviços e produtos, bem como a criação de novos produtos e serviços de forma a proporcionar uma maior qualidade de vida aos cidadãos.

Para tal, vamos estudar a técnica da agregação, de um ponto de vista legal, de forma a compreender se os dados agregados são dados anónimos ou se são subsumíveis ao conceito de dados pessoais constante do RGPD. Isto porque, se os dados agregados forem considerados dados pessoais, ficam sujeitos às exigências do RGPD e, por consequência, tem de ser respeitado o princípio da limitação das finalidades, que não permite o tratamento posterior de forma incompatível com as finalidades que motivaram a recolha (art. 5.º, n.º 1, alínea b) do RGPD).

Para compreendermos os tratamentos de dados pessoais em causa, consideramos essencial a divisão do projeto em duas fases:

a) A fase da recolha e da agregação dos dados (doravante designada de "Fase 1")

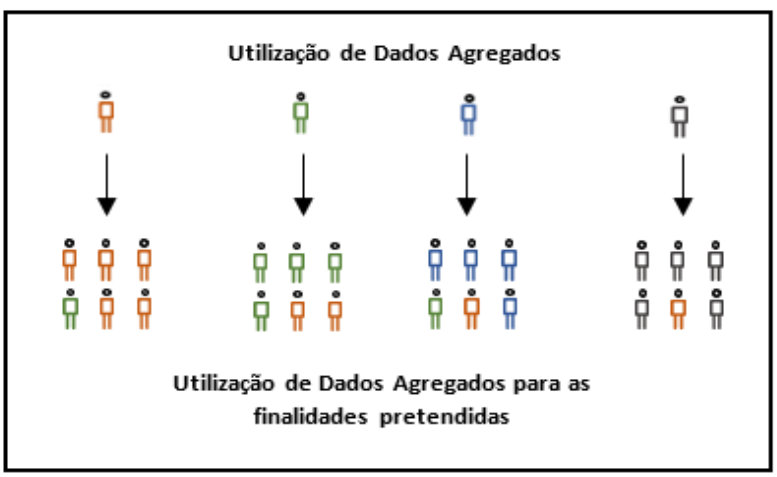
Figura 4 – Recolha e Agregação de Dados (Fase 1)



Fonte: Elaboração própria

b) A fase de utilização dos dados agregados para caracterização de pessoas singulares (doravante designada de "Fase 2")

Figura 5 - Utilização dos dados agregados para caracterização de pessoas singulares (Fase 2)



Fonte: Elaboração própria

A Figura 4 – Recolha e Agregação de Dados representa a Fase 1 do projeto onde os dados pessoais são recolhidos de vários titulares dos dados nos diversos serviços disponibilizados pelos municípios. Nesta fase, os dados são recolhidos, por regra, diretamente do titular dos dados e permitem a identificação do mesmo.

No sentido de proteger a privacidade dos titulares dos dados é utilizada a técnica de agregação de dados onde são obtidas informações sumarizadas. Estas informações sumarizadas não contemplam dados que identifiquem pessoas singulares, constituindo dados de um determinado grupo.

Como exemplo ilustrativo desta primeira fase temos a recolha de dados de consumos de água de uma determinada localidade por habitante para fins de prestação de serviços de fornecimento de água. À partida, estes dados seriam tratados única e exclusivamente para a referida finalidade (i.e., execução do contrato de prestação de serviços de fornecimento de água), contudo, com o

objetivo de otimizar a presente recolha, os dados vão ser objeto de agregação. Os dados obtidos através da técnica de agregação de dados constituem uma referência abstrata que caracteriza todo o conjunto de habitantes da referida localidade.

A Figura 5 - Utilização dos dados agregados para caracterização de pessoas singulares (Fase 2) - representa a fase do projeto onde os dados agregados (i.e., que constituem uma referência abstrata) são utilizados para efeitos de caracterização de uma pessoa singular. Com as referências abstratas obtidas, que caracterizam um grupo de pessoas, pretende-se inferir potenciais comportamentos / decisões dos titulares dos dados. Ora, tendo em consideração que são obtidas referências abstratas, quando relacionadas com pessoas singulares, em regra representam meras probabilidades.

Pegando no exemplo acima apresentado, a referência abstrata obtida, que caracteriza os consumos de água de todo o conjunto de habitantes da referida localidade, vai ser relacionada com pessoas singulares no sentido de procurar prever o seu consumo de água. Através desta relação entre a referência abstrata obtida e uma pessoa singular, em regra, vamos obter uma probabilidade de uma pessoa A ter um determinado consumo.

6.2. Subsunção dos dados agregados ao conceito de dados pessoais

Cumpre agora analisar se os dados agregados (i.e., dados sumarizados) são ou não subsumíveis no conceito de dados pessoais constante do n.º 1 do art. 4.º do Regulamento Geral de Proteção de Dados. Para tal, será necessária a análise dos 5 elementos constantes da definição de dados pessoais, em particular: i) informação; ii) relativa a; iii) uma pessoa singular; iv) identificada; e v) identificável.

Como vimos anteriormente o Regulamento Geral de Proteção de Dados procura oferecer um conceito amplo de dados pessoais, começando por referir que dados pessoais são informações. O conceito de informação não se encontra detalhado no RGPD, sendo comummente entendido como um conjunto de dados organizados que proporcionam sentido e valor para o recetor. Tratando-se de dados agregados constituem necessariamente dados organizados e tratados

que têm valor e sentido quando interpretados, pelo que concluímos que estes dados são considerados informações.

Concluído que os dados agregados são informações cumpre analisar se estas informações são relativas a uma pessoa singular[45]. Para que as informações sejam consideradas dados pessoais é necessário que exista uma relação entre a informação e um determinado sujeito.

Como é referido no n.º 1 do art.1.º, do Regulamento Geral de Proteção de Dados[46], as regras estabelecidas neste visam a proteção de pessoas singulares. Um dos principais objetivos do Regulamento Geral de Proteção de Dados prende-se com a devolução do controlo às pessoas singulares dos seus próprios dados pessoais e, o coração do Regulamento, são os direitos, liberdades e garantias da pessoa singular.

No que concerne aos dados obtidos através da técnica de agregação é necessário compreender a quem pertencem os atributos objeto de agregação, isto é:

> a) A técnica da agregação pode ser aplicada a vários atributos de uma pessoa singular. Nesta situação, os dados agregados obtidos e quando relacionados com a pessoa singular em causa, configuram dados pessoais na medida em que são "*relativos a uma pessoa singular*" sendo esta pessoa singular "*identificada*". Neste caso, quando os atributos objeto de agregação respeitam a uma pessoa singular, os dados agregados constituem dados pessoais, nos termos e para os efeitos do n.º 1 do art. 4.º do RGPD.
>
> b) Quando a técnica da agregação é aplicada aos atributos partilhados por x utilizadores, os dados resultantes da agregação passam a ser dados referentes a um grupo. Neste caso, deixa de ser possível selecionar uma pessoa dentro de um grupo de x pessoas[47]. Ora, se os dados deixam de ser dados relativos a pessoas

45 Cfr. Considerando 14 conjugado com o art. 3.º do RGPD.

46 "O presente regulamento 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 do Regulamento Geral de Proteção de Dados.

47 GT 29, Parecer 05/2014, cit., 18.

singulares e passam a ser dados relativos a grupos de pessoas, não são subsumíveis ao conceito de dados pessoais constante do RGPD.

Nesta última situação, poderá colocar-se a questão de o número de pessoas (x) ser um valor baixo. É importante notar que, quanto maior é o número de pessoas, maior é a privacidade e menor é a taxa de sucesso em caso de tentativa de re-identificação. No entanto, tendo em consideração que o objeto de análise é a possibilidade de subsunção ao conceito de dados pessoais que nos é apresentado pelo RGPD, desde que o x seja superior ou igual a 2, os dados são considerados dados anónimos.

Adicionalmente, é necessário analisar se uma probabilidade de determinado dado agregado pertencer a uma determinada pessoa é ou não é um dado pessoal. Atualmente, já existem variados estudos que permitem o cálculo da probabilidade de determinado *data set* agregado ser objeto de re-identificação. A questão que se coloca neste âmbito é se obtivermos uma probabilidade de 10% ou de 90% de determinado dado agregado pertencer a um perfil de uma pessoa singular e identificá-la, é ou não dado pessoal.

Para verificarmos a subsunção ao conceito será necessário relembrar que o Regulamento considera dados pessoais as informações relativas a uma pessoa singular identificada ou identificável, sendo identificável uma pessoa singular que possa ser identificada, direta ou indiretamente. A letra da lei é clara quando refere que, para que determina informação seja considerada um dado pessoal, é necessário que a mesma permita identificar uma pessoa direta ou indiretamente.

Assim sendo, nos casos em que exista uma determinada probabilidade de um perfil pertencer a uma determinada pessoa, não poderá ser considerado um dado pessoal, quer se trate de uma probabilidade de 10% ou de 90%. Isto porque, independentemente da probabilidade em causa, é sempre um dado relativo a um grupo de pessoas. Para além de ser um dado de um grupo de pessoas, não constituí uma informação relativa a uma pessoa "*identificada ou identificável*".

Neste sentido, concluímos que sempre que tenhamos uma probabilidade de identificação, independentemente de qual for, nunca será subsumível ao

conceito de dados pessoais constante do Regulamento Geral de Proteção de Dados.

Ora, a partir do momento em que deixamos de ter uma probabilidade e passamos a ter uma certeza na identificação de uma pessoa singular, os dados agregados passam a ser dados pessoais para efeitos do Regulamento Geral de Proteção de Dados.

Assim sendo, os dados agregados são considerados dados anónimos quando calculados com base em atributos de um grupo de pessoas e quando existam apenas probabilidades de identificação de uma pessoa singular.

6.3. Os tratamentos de dados no âmbito das Smart Cities

Passemos agora para a análise dos tratamentos de dados no âmbito das Smart Cities, ou seja, no âmbito das fases acima identificadas (i.e., Fase 1 e Fase 2). O objetivo pretendido é compreender em que momentos estamos perante dados pessoais, nos termos do n.º 1 do art. 4.º do Regulamento Geral de Proteção de Dados.

A primeira fase do projeto é caracterizada pela recolha de dados pessoais dos cidadãos que é levada a cabo pelos municípios, em particular, no âmbito da gestão dos serviços públicos. Relativamente a este primeiro momento da primeira fase do projeto, não existem dúvidas de que estamos perante dados subsumíveis ao conceito de dados pessoais. As informações recolhidas por parte dos municípios respeitam a pessoas singulares, sendo possível identificar diretamente as mesmas.

De seguida, ainda dentro desta primeira fase, os dados respeitantes a pessoas singulares são objeto de agregação. Através desta técnica, os dados são agregados por x indivíduos, constituindo sempre dados relativos a um grupo de pessoas. Ora, se são dados relativos a um grupo de pessoas não respeitam uma pessoa singular.

No contexto das *Smart Cities*, os dados agregados respeitam sempre a grupos de pessoas, não se colocando a questão levantada de se tratarem de vários atributos pertencentes a uma pessoa.

Na segunda fase, ilustrada na figura 5, os dados obtidos através do processo de agregação na fase 1, são relacionados com pessoas singulares. Exemplo desta situação ocorre quando se obtém uma referência abstrata relativa ao consumo de água de um determinado grupo de pessoas e esse consumo é relacionado com uma determinada pessoa singular de forma a obter uma probabilidade da mesma ter o referido consumo.

Neste caso é necessário distinguir as situações em que, através da relação entre os dados agregados e uma pessoa singular, se obtém uma probabilidade ou uma certeza sobre a mesma. Como vimos anteriormente, sempre que se obtenham probabilidades sobre um dado poder pertencer a determinada pessoa, independentemente de qual for a probabilidade, nunca são dados pessoais. Estes dados não são pessoais na medida em que não são "*dados relativos a uma pessoa singular*". Contudo, nas situações em que obtemos certezas sobre uma pessoa singular, passamos a ter "*dados relativos a uma pessoa singular identificada*".

Em suma, analisadas as duas fases do projeto, apenas no momento inicial de recolha de dados estaremos perante dados pessoais. O único momento em que voltamos a ter dados pessoais é quando relacionamos os dados agregados com as pessoas singulares e obtermos certezas sobre as mesmas.

7. Conclusão

O presente estudo foi despoletado pela verificação atual de uma recolha massiva de dados pessoais dos munícipes, bem como o desenvolvimento de tecnologias de informação que permitem ainda uma recolha de maior qualidade, quantidade e variedade. Através desta verificação, foi percecionada a necessidade de uma solução que visasse otimizar a recolha de dados, de forma a prestar um melhor serviço público.

Neste contexto, através do presente estudo, procurámos encontrar um critério legal que permitisse concluir a partir de que momento os dados agregados são considerados dados anónimos[48]. A procura desta solução visa

48 Cfr. art. 1.º, 2.º e 3.º e considerando 26 do Regulamento Geral de Proteção de Dados.

permitir que as cidades utilizem os dados recolhidos sem colocar em causa a privacidade dos cidadãos.

Nesta análise concluímos que os dados agregados são dados anónimos quando sejam calculados com base em atributos de um grupo de pessoas e quando exista apena uma probabilidade de identificação de uma pessoa singular.

Concluímos ainda que, através deste critério será possível que as cidades inteligentes otimizem a utilidade dos dados já recolhidos, não sendo necessário o cumprimento do Regulamento Geral de Proteção de Dados e não ficando sujeito ao princípio da limitação das finalidades.

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 catorze investigadores (quatro doutorados) oriundos de faculdades de direito (professores e doutorandos), de empresas e do setor público.

Os sete artigos publicados na edição de 2022 do Anuário resultam de uma chamada lançada em outubro de 2021. Os textos foram sujeitos a um processo de blind peer review, e posteriormente revistos pelos coordenadores do Anuário.

JURIS NOVA
DataporEU
SRS ADVOGADOS FOCUS MATTERS.
FUTURA