CENTRO DE ESTUDOS JUDICIÁRIOS

Coleção Formação Contínua

Direito à Informação Administrativa e Proteção de Dados Pessoais

Jurisdição Administrativa e Fiscal

outubro 2021

CENTRO DE ESTUDOS JUDICIÁRIOS

Diretor do CEJ
João Manuel da Silva Miguel, Juiz Conselheiro

Diretores Adjuntos
Luís Manuel Cunha Silva Pereira, Procurador-Geral Adjunto
José Eduardo Sapateiro, Juiz Desembargador

Coordenadora do Departamento da Formação
Carla Câmara, Juíza Desembargadora

Coordenadora do Departamento de Relações Internacionais
Helena Leitão, Procuradora da República

Grafismo
Ana Caçapo - CEJ

Capa
Bancos no edifício do CEJ

Foto
Paulo Rainho - CEJ

A jurisdição administrativa tem organizado sucessivas ações de formação contínua sobre o direito à informação administrativa e proteção de dados, o que tem permitido uma reflexão aprofundada sobre tão importante e relevante tema, designadamente no contencioso administrativo.

A pertinência de tais reflexões ganhou ainda maior relevo com a aplicação, a partir de maio de 2018, do Regulamento Geral de Proteção de Dados e, depois, da Lei n.º 58/2019 de 8 de agosto, que assegurou a execução daquele Regulamento na ordem jurídica nacional.

No presente e-book reúnem-se alguns textos elaborados pelos reputados oradores a pedido do CEJ, na sequência das comunicações que tiveram lugar nas ações de formação contínua organizadas sobre o tema, que decorreram em julho de 2018 e junho e dezembro de 2019.

Permite-se assim um amplo acesso ao conhecimento das reflexões então feitas e entretanto plasmadas por escrito.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

Ficha Técnica

Nome:

Direito à Informação Administrativa e Proteção de Dados Pessoais

Jurisdição Administrativa e Fiscal:

Fernando Duarte – Juiz Desembargador, Docente do CEJ e Coordenador da Jurisdição
Marta Cavaleira – Juíza Desembargadora e Docente do CEJ
Ana Carla Duarte Palma – Juíza Desembargadora e Docente do CEJ
Tiago Brandão de Pinho – Juiz de Direito e Docente do CEJ
Filipe Duarte Neves – Juiz de Direito e Docente do CEJ

Coleção:

Formação Contínua

Plano de Formação 2019/2020:

A tutela urgente no contencioso administrativo – 12 e 13 de dezembro de 2019 (programa)

Plano de Formação 2018/2019:

Proteção de Dados Pessoais – 19 de junho de 2019 (programa)

Plano de Formação 2017/2018:

Direito de Informação Administrativa e Proteção de Dados – 6 de julho de 2018 (programa)

Intervenientes:

Graça Canto Moniz – Professora da Faculdade de Direito da Universidade Lusófona, Professora convidada da Nova *School of Law*
Teresa Coelho Moreira – Professora da Escola de Direito da Universidade do Minho. Membro da Direção da APODIT – Associação Portuguesa de Direito do Trabalho. Membro integrado do JusGov – Centro de Investigação em Justiça e Governação e Coordenadora do Grupo de Investigação em Direitos Humanos do mesmo
Ana Fernanda Neves – Professora da Faculdade de Direito da Universidade de Lisboa
Alessandra Silveira – Professora da Escola de Direito da Universidade do Minho e Diretora do Mestrado em Direito da União Europeia. Titular da Cátedra Jean Monnet em Direito da União Europeia
Joana Covelo de Abreu – Professora da Escola de Direito da Universidade do Minho e da Universidade Portucalense Infante D. Henrique. Coordenadora do Módulo *Jean Monnet eUjust* "EU Procedure and credits' claims: approaching electronic solutions under e-Justice paradigm" (2019-2022)
Tiago Sérgio Cabral – Advogado
Tiago Fidalgo de Freitas – Assistente convidado da Faculdade de Direito da Universidade de Lisboa; investigador associado e coordenador executivo do CIDP – Centro de Investigação de Direito Público; consultor coordenador do Centro de Competências Jurídicas do Estado (JurisAPP)
Nuno Sousa e Silva – Professor na Faculdade de Direito da Universidade Católica Portuguesa, Porto

Revisão final:
Carla Câmara – Juíza Desembargadora, Coordenadora do Departamento da Formação do CEJ

Notas:

Para a visualização correta dos e-books recomenda-se o seu descarregamento e a utilização do programa Adobe Acrobat Reader.

Foi respeitada a opção dos autores na utilização ou não do novo Acordo Ortográfico.

Os conteúdos e textos constantes desta obra, bem como as opiniões pessoais aqui expressas, são da exclusiva responsabilidade dos/as seus/suas Autores/as não vinculando nem necessariamente correspondendo à posição do Centro de Estudos Judiciários relativamente às temáticas abordadas.

A reprodução total ou parcial dos seus conteúdos e textos está autorizada sempre que seja devidamente citada a respetiva origem.

Forma de citação de um livro eletrónico (NP405-4):

AUTOR(ES) – **Título** [Em linha]. a ed. Edição. Local de edição: Editor, ano de edição.
[Consult. Data de consulta]. Disponível na internet: <URL:>. ISBN.

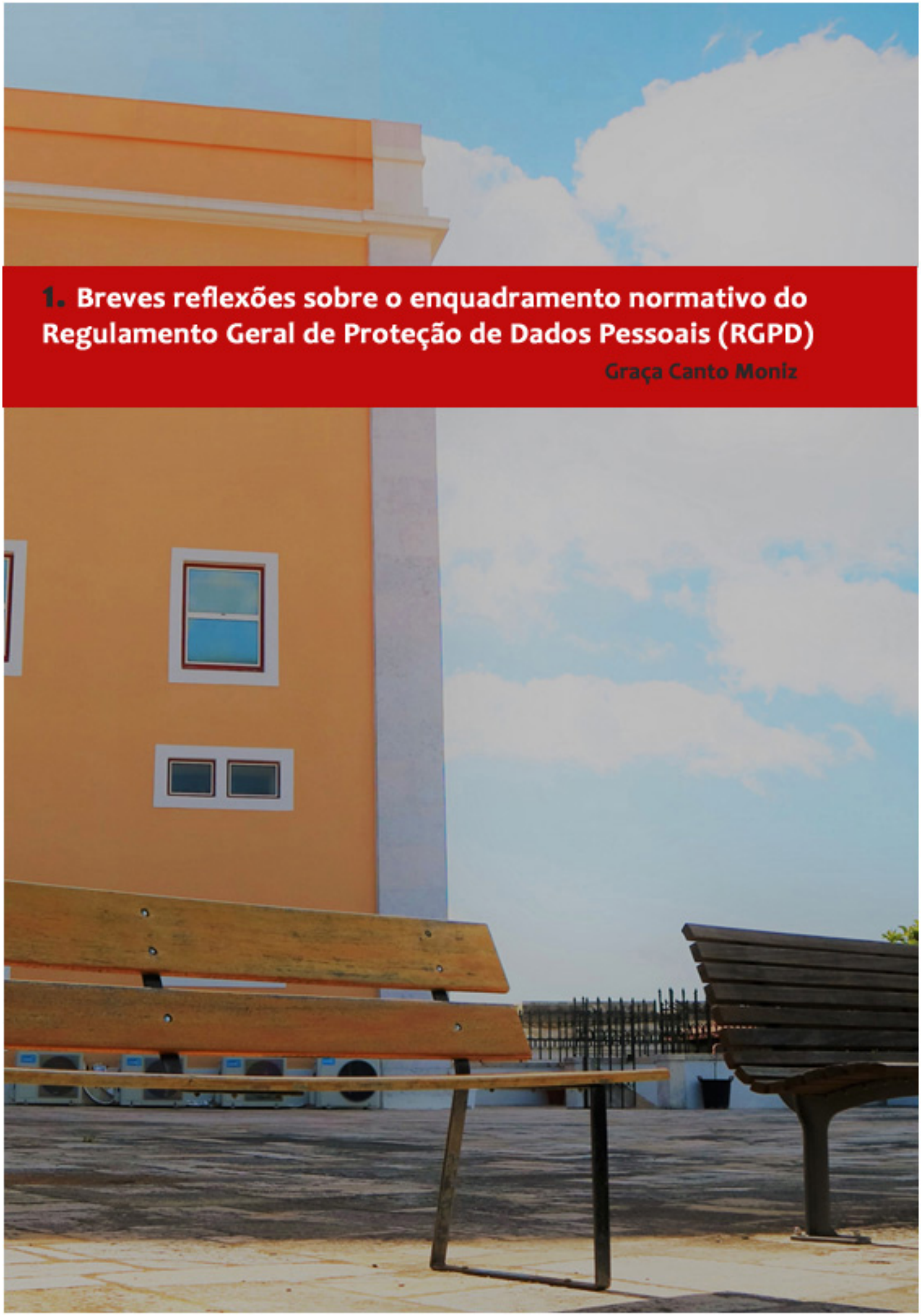
Exemplo:
Direito Bancário [Em linha]. Lisboa: Centro de Estudos Judiciários, 2015.
[Consult. 12 mar. 2015].
Disponível na
internet: <URL: http://www.cej.mj.pt/cej/recursos/ebooks/civil/Direito_Bancario.pdf.
ISBN 978-972-9122-98-9.

Registo das revisões efetuadas ao e-book

Identificação da versão	Data de atualização
06/10/2021	11/10/2022
	12/10/2022

DIREITO À INFORMAÇÃO ADMINISTRATIVA E PROTEÇÃO DE DADOS PESSOAIS

Índice



1. Breves reflexões sobre o enquadramento normativo do Regulamento Geral de Proteção de Dados Pessoais (RGPD)

Graça Canto Moniz

CENTRO
DE ESTUDOS
JUDICIÁRIOS

1. BREVES REFLEXÕES SOBRE O ENQUADRAMENTO NORMATIVO DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS PESSOAIS (RGPD)*

Graça Canto Moniz**

O Regulamento geral de proteção de dados pessoais[1] ("RGPD") não é um diploma de fácil compreensão e aplicação. A sua extensão (99.º artigos e 173 considerandos) não facilita a tarefa do aplicador ao que acresce, por um lado, o conteúdo (permeado por conceitos indeterminados e por um conjunto de imposições novas para os responsáveis pelo tratamento e subcontratantes) e, por outro, a sua intrigante natureza jurídica.

É sobre este último aspeto que me vou debruçar neste texto. Para tanto analisarei dois pontos do esquema normativo subjacente ao RGPD:

> (1) A "europeização" da proteção de dados pessoais e as duas dimensões da mesma e
> (2) A natureza jurídica da matéria da proteção de dados pessoais propriamente dita, procurando saber se lidamos com Direito Público, Direito Privado e questionando se faz sentido aplicar essa tipologia àquela matéria.

1. A "europeização" da proteção de dados pessoais

O fenómeno da "europeização" de certas matérias corresponde ao papel principal do Direito da União Europeia ("DUE") enquanto fonte do direito aplicável e desdobra-se, essencialmente, em dois vetores:

> (i) A sua influência na homogeneização dos regimes jurídicos aplicáveis nos Estados-Membros e
> (ii) A estruturação de um sistema administrativo europeu que conjuga degraus ou níveis de administração[2]. O regime em análise reúne estes dois elementos.

---

* Apresentação decorrente da ação de formação contínua do CEJ "Direito de Informação Administrativa e Proteção de Dados", realizada a 6 de julho de 2018.

** Professora da Faculdade de Direito da Universidade Lusófona, Professora convidada da Nova *School of Law*.

[1] Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[2] Alexandre Dias PEREIRA, *Direitos de Autor e Liberdade de Informação*, Almedina, 2008, p. 344 e ss.; Maria Eduarda GONÇALVES, *Direito da Informação – Novos Direitos e Formas de Regulação na Sociedade da Informação*, 2ª ed.,

Enquanto competência atribuída à União Europeia ("UE"), entre 1995 e a atualidade, a matéria da proteção de dados pessoais sofreu uma evolução patente no direito derivado e no direito originário. É um percurso pontuado pelos avanços genéticos da UE e pela dinâmica própria da sua vivência, destacando-se a harmonização de divergências nacionais entre Estados-Membros, o florescimento de uma economia de mercado e a consciencialização da necessidade de conferir maior centralidade aos direitos fundamentais no seio da União. É assim que, aos olhos da Comissão Europeia, este regime consagra "duas das mais antigas e igualmente importantes ambições do processo de integração europeia": a proteção dos direitos fundamentais e a realização do mercado interno, em especial a livre circulação de dados pessoais[3]. Desta afirmação retiram-se as duas dimensões deste bloco normativo, uma jusfundamental e outra económica ou "integracionista", correspondentes aos objetivos enunciados no art. 1.º do RGPD e da Diretiva que o antecedeu[4].

1.1. A dimensão económica ou "integracionista"

A década de 70 foi marcada pelo surgimento das primeiras legislações nacionais de proteção de dados pessoais[5]. Tal fez soar o alerta, junto da Comissão Europeia, de que os Estados-Membros estavam na eminência de adotar soluções divergentes[6]. A toada fez eco no Parlamento Europeu que, entre 1975 e 1982, discutiu quatro resoluções nas quais se antecipava o surgimento de legislação conflituante e os efeitos negativos no desenvolvimento de um mercado comum, apelando-se à criação de um mercado comum de proteção de dados pessoais de modo a garantir a livre circulação de informação na UE. Invocava-se, para fundamentar a respetiva competência, o art. 100.º dos Tratados (hoje o art. 114.º do Tratado de Funcionamento da União Europeia ou "TFUE"[7]), e o imperativo de aproximar legislações nacionais[8].

Almedina, 2003, p. 30; Paulo OTERO, *Legalidade e Administração Pública – O sentido da vinculação administrativa à juridicidade*, Almedina, 2003, p. 231 e ss.; Pedro GONÇALVES, "Direito Administrativo da Regulação", *Regulação, Electricidade e Telecomunicações*, Coimbra Editora, 2008, p. 31; Yves POULLET, "Vers la confiance: vues de Bruxelles: un droit européen de l'Internet? Quelques considérations sur la spécificité de l'approche réglementaire européene du cyberspace", Georges CHATILLON, (org.), *Le droit international de l'Internet*, 2002, p. 133 e ss..

[3] Comissão Europeia, "Uma abordagem global da proteção de dados pessoais na União Europeia", 4 de novembro de 2010, p. 2.

[4] O art. 1.º, n.º 1, da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995 (doravante "Diretiva"), relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, dispunha que "Os Estados-membros assegurarão, em conformidade com a presente directiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais." (dimensão jusfundamental). Por seu turno, o número 2, referia que "os Estados-membros não podem restringir ou proibir a livre circulação de dados pessoais entre Estados-membros por razões relativas á proteção assegurada por força do n.º 1" (dimensão integracionista). Já o art. 1.º, n.º 2, do RGPD enuncia que "O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais" (dimensão jusfundmanental). Por seu turno, o número 3, refere que "A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais" (dimensão integracionista).

[5] Em 1970 no Estado Alemão de Hesse, em 1973 na Suécia, em 1977 e 78, respetivamente, na Alemanha e em França, v. Gloria FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Springer, 2014, p. 19 e ss..

[6] Comissão Europeia, "Community policy on data processing", novembro de 1973, p. 13.

[7] Cuja epígrafe é "a aproximação de legislações".

[8] Sobre estas resoluções, v. G. FUSTER, *The Emergence of* cit., p. 115 e ss..

Estes receios ganharam vida quando as autoridades nacionais restringiram os fluxos de dados pessoais entre Estados-Membros, fluxos esses essenciais para empresas estabelecidas em mais do que um. Por exemplo, em 1989 a autoridade de controlo francesa ("CNIL") bloqueou a transmissão dos dados pessoais de um colaborador do escritório da *Fiat*, em Paris, para o escritório de Turim, em Itália, invocando lacunas no direito da proteção de dados pessoais italiano[9]. Tornava-se evidente que a livre circulação de dados pessoais, essencial para um mercado que se pretendia sem fronteiras, requeria um ato legislativo da UE no sentido de harmonizar legislações e remover obstáculos à circulação dos dados pessoais[10]. Por conseguinte, em 1990, a Comissão Europeia apresentou uma proposta de Diretiva[11] ("proposta original"), alterada em 1992[12] ("proposta alterada"), inspirada na Convenção n.º 108 do Conselho da Europa, na legislação federal alemã e francesa[13]. As descrições doutrinais da Diretiva 95/46 ("Diretiva") como uma ferramenta de neutralização da soberania nacional em favor da eficiência económica giram à volta desta dimensão integracionista[14].

O propósito harmonizador do RGPD ou a "dimensão mercado único" são declarados nas comunicações da Comissão Europeia que antecederam a sua adoção, nos considerandos, e implícitos em várias disposições[15]. Por um lado, no art. 51.º, n.º 2, nos termos do qual as autoridades de controlo devem contribuir para a "aplicação coerente" do RGPD e, por outro lado, em três mecanismos especificamente arquitetados para esse fim: o mecanismo *one-stop-shop*[16] ou sistema de balcão único, a cooperação entre autoridades de controlo[17] e o procedimento de controlo da coerência[18]. Adicionalmente, o art. 92.º e os considerandos 167 a 169, atribuem poderes executivos à Comissão Europeia para orientar a aplicação de certas normas.

[9] CNIL, "Délibération n.º 89/78 du 11 juillet 1989", *Dixième Rapport au Président de la République et au Parlement,* 1989, p. 32 e ss.. Mas há outros exemplos: na década de 70 a autoridade nacional Sueca recusou a transmissão de dados pessoais para o Reino Unido em vários casos; em 1980 a Áustria adotou legislação que exigia a autorização prévia do Comissário Austríaco de Proteção de Dados antes da transmissão de dados sobre pessoas coletivas para certos Estados-Membros uma vez que a legislação de proteção de dados desses países não abrangia aquele tipo de dados, v. Christopher KUNER, *Transborder Data Flows and Data Privacy Law,* Oxford University Press, 2013, p. 40 e Jon BING, *Transnational Data Flows and the Scandinavian Data Protection Legislation*, Stockholm Institute for Scandinavian Law, 1980, p. 73.

[10] G. FUSTER, *The Emergence of* cit., p. 126; Helmut HEIL, "Directive 95/46/EC of the European Parliament and of the Council: Introductory remarks", Alfred BULLESBACH *et alii*, *Consice European IT Law (Second Edition),* Kluwer Law International, 2010, p. 10 e María del Carmen GUERRERO, *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal,* Thomson Civitas, 2006, p. 61.

[11] Proposta de diretiva do Conselho relativa à proteção das pessoas no que diz respeito ao tratamento dos dados pessoais, 24 de setembro de 1990.

[12] Proposta alterada de diretiva do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à sua livre circulação, 18 de outubro de 1992.

[13] G. FUSTER, *The Emergence of* cit., p. 126

[14] O. LYNSKEY, *The Foundations* cit., p. 50.

[15] Comissão Europeia, "Proteção da privacidade num mundo interligado. Um quadro europeu de proteção de dados para o século XXI", 25 de janeiro de 2012, p. 8 e 9 e "Uma abordagem..." cit., p. 10; considerandos 7, 9 e 10 do RGPD.

[16] Para os casos de "tratamento transfronteiriço", definido nos termos do art. 4.º, n.º 23, quando existe uma "autoridade de controlo principal", de acordo com o art. 56.º. A ideia é que os responsáveis pelo tratamento tenham apenas uma única autoridade de controlo como interlocutor.

[17] Artigos 60.º e ss..

[18] Artigos 63.º e ss.. Este mecanismo visa assegurar que as decisões de uma autoridade de controlo com impacto a nível europeu tenham em conta os pareceres emitidos pelas outras autoridades interessadas e sejam conformes com o DUE.

A dimensão integracionista poderá ser prejudicada, por exemplo, pela margem de manobra concedida ao direito nacional em certos domínios, pelas divergências interpretativas ainda existentes entre autoridades de controlo ou pela falta de recursos e meios de algumas autoridades por comparação com outras[19]. Por isso compreendo aqueles que invocam F. CARNELUTTI para considerar que o RGPD tem "o corpo de um regulamento, mas a alma de uma diretiva"[20].

1.2. A dimensão jusfundamental

Recordando o pendor maioritariamente económico dos primeiros passos da integração europeia, à data de adoção da Diretiva o relevo dos direitos fundamentais no projeto europeu era menor[21]. Em todo o caso, todos os intervenientes do processo legislativo de redação daquele diploma expressaram, desde o início, preocupações com os riscos para os direitos fundamentais oriundos dos novos tratamentos de dados pessoais desencadeados pelo desenvolvimento tecnológico. Em várias resoluções do Parlamento Europeu, entre 1975 e 1982[22], a preocupação é manifesta, bem como na Comunicação da Comissão Europeia anexa à primeira proposta de Diretiva, onde se constata que a legislação nacional em vigor nos Estados-Membros é deficiente e "não reflete o compromisso da Comunidade com a proteção dos direitos fundamentais"[23].

No passado, alguns autores enquadraram este bloco normativo numa tendência específica do DUE segundo a qual os direitos fundamentais seriam "trunfos" contra as liberdades do mercado interno[24]. Outros defendiam que este regime seria "consistente com uma conceção de privacidade informacional enquanto direito fundamental"[25]. O Tribunal de Justiça ("TJ") declarou, em 2003, no caso *Rundfunk*[26], que a Diretiva devia ser interpretada à luz dos direitos fundamentais. Porém, foi o Tratado de Lisboa ("TL") que firmou a dimensão jusfundamental deste regime, em especial o art. 16.º do TFUE e o art. 8.º da Carta dos Direitos Fundamentais

[19] E Autoridade Europeia de Proteção de Dados Pessoais, "Opinion of the European Data Protection Supervisor on the Data Protection Reform Package", 7 de março de 2012, p. 9. Apesar de incidir sobre a primeira proposta do RGPD da Comissão Europeia, muitas dos alertas ali lançados são válidos para a versão final do RGPD, v. Christopher KUNER, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", *Bloomberg BNA Privacy and Security Law Report,* 6 de fevereiro de 2012, p. 13 e O. LYNSKEY, *The Foundations of* cit., p. 73.

[20] Pablo MEXÍA, "La singular naturaleza jurídica del reglamento general de protección de datos de la UE. Sus efectos en acervo nacional sobre protección de datos", *Reglamento General De Protección De Datos. Hacia um nuevo modelo europeo de privacidade,* José Piñar MAÑAS (dir.), Reus, 2016, p. 34.

[21] G. FUSTER, *The Emergence of* cit., p. 126.

[22] A própria designação destas resoluções é esclarecedora: "Resolução sobre a proteção dos direitos do indivíduo em face dos desenvolvimentos tecnológicos no domínio da proteção de dados pessoais".

[23] Comissão Europeia, "Comunicação relativa à proteção das pessoas no que diz respeito ao tratamento dos dados pessoais na Comunidade e à segurança dos sistemas de informação, 24 de setembro de 1990, p. 15.

[24] G. FUSTER, *The Emergence of* cit., p. 135 e John MORIJN, "Balancing Fundamental Rights and common market freedoms in Union Law: Schmidberger and Omega in the light of the European Constitution", *European Law Journal,* vol. 12, n.º 1, 2006, p. 15.

[25] Pamela SAMUELSON, "Privacy as Intellectual Property", *Standford Law Review,* n.º 52, 2000, p. 1125 e ss..

[26] "Cabe ainda acrescentar que as disposições da Diretiva 95/46, na medida em que regulam o tratamento de dados pessoais suscetíveis de pôr em causa as liberdades fundamentais e, em especial, o direito à vida privada, devem necessariamente ser interpretadas à luz dos direitos fundamentais (...)", Acórdão do TJ Österreichischer Rundfunk et alii c. Christa Neukomm e Joseph Lauermann, C-465/00, 20 de maio de 2003, n.º 68.

da União Europeia ("CDFUE"), no seguimento de recomendações de várias entidades[27]. Redigidos em termos semelhantes, os dois artigos reconhecem que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhe digam respeito".

As consequências desta "constitucionalização"[28] da proteção de dados pessoais fazem-se sentir a vários níveis: desde logo, na jurisprudência do TJ – acusado por alguns autores de "ativismo judicial"[29] – bem como na autonomização do direito à proteção de dados pessoais do direito ao respeito pela vida privada e familiar consagrado no art. 7.º da CDFUE.

Com efeito, no passado, alguns autores consideraram que a proteção concedida aos direitos fundamentais pelo TJ era minimalista e instrumentalizada em função dos objetivos da UE[30]. Não é, de todo, o caso do domínio em estudo em relação ao qual aquela instância tem vindo a posicionar-se como líder na solução dos problemas únicos de proteção da pessoa singular no mundo digital[31]. Em várias ocasiões o art. 8.º da CDFUE e o art. 16.º do TFUE constaram do argumentário do TJ para atribuir prioridade ao direito à proteção de dados pessoais quando ponderado em situações de colisão ou conflito com outros direitos, valores e interesses[32]. Por exemplo, no caso *Google Spain* o TJ declarou que o direito à proteção de dados pessoais prevalece "em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse [do] público em encontrar a referida informação durante uma pesquisa sobre o nome dessa pessoa"[33]. O tribunal advogou a "não subordinação dos direitos fundamentais dos titulares dos dados pessoais a um entendimento superlativo dos interesses económicos dos prestadores de serviços, da liberdade de expressão e dos direitos dos internautas"[34].

[27] Como, por exemplo, do G29, "Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights", 7 de setembro de 1999, p. 2 ou de um grupo de peritos num relatório para a Comissão Europeia, Expert Group on Fundamental Rights, "Affirming fundamental rights in the European Union: time to act", 1999, disponível online em http://ftp.infoeuropa.eurocid.pt/database/000038001-000039000/000038827.pdf , consultado no 30 de setembro de 2018.
[28] O. Lynskey, *The Foundations of* cit., p. 87.
[29] O que, em bom rigor e verdade, não se verifica apenas no domínio da proteção de dados pessoais, v. Graça Moniz, "Compreender o ativismo judicial do Tribunal de Justiça da União Europeia. A "Explicação" de Ronald Dworkin", *Themis,* ano XVIII, n.º 32, 2017, p. 125 e ss..
[30] Catarina Sampaio Ventura, "Contexto e Justificação da Carta", *Carta dos Direitos Fundamentais da União Europeia,* Coimbra Editora, 2001, p. 46.
[31] Frederico Fabbrini, "The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court", Sybe de Vries (ed.), *Five Years of Legally Binding Charter of Fundamental Rights,* Hart Publishing, 2015; Gabriela Zanfir, "How CJEU's 'Privacy Spring' Construed the Human Rights Shield in the Digital Age", *European judicial systems as a challenge for democracy,* Intersentia, 2015, p. 111; Maja Brkan, "The Unstoppable Expansion of the EU Fundamental Right to Data Protection. Little Shop of Horrors?", *Maastricht Journal of European and Comparative Law,* n.º 23, 2016, p. 812 e ss.; Selena Crespi, "Diritti fondamentali, Corte di giustizia e riforma del Sistema UE di protezione dei dati", *Rivista Italiana Di Diritto Pubblico Comunitario,* 2015, p. 819 e ss..
[32] F. Fabbrini, "The EU Charter …" cit., p. 20; M. Brkan, "The Unstoppable …" cit., p. 824 e Mistale Taylor, "The EU's human rights obligations in relation to its data protection laws with extraterritorial effect", *IDPL,* vol. 5, n.º 4, 2015, p. 247 e 253.
[33] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, C-131/12, 13 de maio de 2014, n.º 97.
[34] Catarina Sarmento e Castro, "A jurisprudência do Tribunal de Justiça da União Europeia, o Regulamento Geral sobre a proteção de dados pessoais e as novas perspetivas para o direito ao esquecimento na Europa", *Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos*, Vol. 1, 2016, p. 1061.

O art. 8.º da CDFUE surge também em juízos de ponderação com interesses de segurança e de aplicação da lei, como evidenciam o caso *Digital Rights Ireland*[35], o caso *Schrems*[36], e a opinião do TJ sobre o acordo entre a UE e o Canadá a propósito dos dados de registo de passageiros ou "PNR"[37].

À luz do relevo crescente da proteção de dados pessoais na jurisprudência do TJ, seja para reforçar a tutela da pessoa singular no contexto digital (*Google Spain*), seja como *wake up call*[38] ou reação ao alarme social surgido com as revelações de Edward Snowden, em 2013, com as tendências de *dataveillance* ou *data surveillance*[39] e as derivas securitárias (*Digital Rights Ireland, Schrems* e PNR), há quem observe a emergência de um "super direito"[40] ou "direito pesado"[41]. Outros autores criticam o *data protection activism*[42] do TJ vaticinando consequências nefastas na promoção e proteção de outros direitos, valores e interesses[43]. Por outro lado, o vanguardismo do TJ na regulação da era digital não é uma tarefa fácil e decisões disruptivas como *Google Spain* e *Schrems,* geram questões deixadas em aberto pelo poder judicial que, ainda por cima, teima em prosseguir um estilo minimalista[44]. Há mesmo quem note que, em certos casos, o TJ se limitou a abrir uma caixa de pandora[45].

Além da jurisprudência, a valorização crescente da dimensão jusfundamental deste regime salta à vista nas duas comunicações da Comissão Europeia que antecederam a adoção do RGPD. Ambas enunciam, entre os objetivos principais, o reforço dos direitos fundamentais das

[35] Acórdão do TJ, Digital Rights Ireland *et alii* c. Minister for Communications, Marine and Natural Resources *et alii,* C-293/12, 8 de abril de 2014. Sobre esta decisão, v. F. FABBRINI, "The EU Charter …" cit., p. 19.
[36] Analisado na Parte III, Capítulo 2, ponto 2.3.1. deste trabalho.
[37] Parecer 1/15 do TJ, ECLI:EU:C:2017:592; Desenvolvendo as implicações deste parecer, v. Christopher KUNER, "Court of Justice International agreements, data protection, and fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR", *Common Market Law Review*, vol. 55, n.º 3, 2018, p. 857 e ss..
[38] Anna DIMITROVA, "Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair", *Journal of Common Market Studies,* vol. 56, 2018 e Tuomas OJANEN, "Privacy is More than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance", *European Constitutional Law Review,* n.º 10, 2014, p. 528.
[39] Como refere M. TZANOU as medidas de "vigilância dos dados" partilham o mesmo *modus operandi*: prosseguem a luta contra a criminalidade grave e a prevenção de crimes transnacionais; implicam a cooperação forçada de atores privados e a recolha de um volume significativo de dados pessoais; os dados pessoais são tratados e usados de forma probabilística e algorítmica, v. Maria TZANOU, *The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance,* Hart Publishing, 2017, p. 251.
[40] Christopher KUNER, "A Super-Right to Data Protection? The Irish Facebook Case and the Future of EU Data Transfer Regulation", *LSE Media Policy Project Blog,* Dezembro de 2014, disponível em http://blogs.lse.ac.uk/mediapolicyproject/2014/06/24/a-super-right-to-data-protection-the-irish-facebook-case-the-future-of-eu-data-transfer-regulation/, consultado no 30 de setembro de 2018.
[41] M. TAYLOR, "The EU's human rights …" cit., p. 254.
[42] M. TZANOU, *The Fundamental* cit., p. 63.
[43] M. TAYLOR dá o exemplo da China e a Rússia, países com regimes de privacidade rigorosos e *firewalls* na Internet que conflituam com a liberdade de expressão e com a livre circulação da informação, v. "The EU's human rights …" cit., p. 255, nota de rodapé 86. No mesmo sentido, Bilyana PETKOVA, "Towards na Internal Hierarchy of Values in the EU Legal Order: Balancing the Freedom of Speech and Data Privacy", *Maastricht Journal of European and Comparative Law,* vol. 23, n.º 3, 2016 e F. FABBRINI, "The EU Charter …" cit., p. 20, remetendo para bibliografia sobre estes "dilemas constitucionais" e M. BRKAN, "The Unstoppable..." cit., p. 827, alertando para o surgimento de desequilíbrios na proteção dos direitos fundamentais na UE.
[44] Christopher KUNER, "The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines", Burkhard HESS e Cristina MARIOTTINI, (eds.), *Protecting Privacy in International and Procedural Law and By Data Protection (European and American Developments),* Ashgate-Nomos, 2015, p. 19 e ss.; Gráinne DE BURCA, "After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?", *MJECL*, n.º 168, 2013, p. 184; Joseph WEILER, "The Judicial Après Nice", Gráinne DE BURCA e Joseph WEILER (eds), *The European Court of Justice,* 2001, Oxford University Press, p. 215 e 224.
[45] F. FABBRINI, "The EU Charter …" cit., p. 21.

pessoas singulares, em especial o direito à proteção de dados pessoais, um imperativo em face de um contexto digital que coloca novos desafios e riscos[46]. Acresce que aquele diploma, por contraposição com a Diretiva, autonomizou dos demais o direito fundamental à proteção de dados pessoais[47] e reforçou os direitos do titular dos dados pessoais, criando novos trunfos para este, como, por exemplo, o direito à portabilidade[48].

2. A complexidade da natureza jurídica da proteção de dados pessoais

Neste segundo ponto começo por avaliar se é ou não possível e adequado "encaixar" esta matéria nalgum dos tradicionais ramos do direito (2.1.). De seguida, sugiro uma perspetiva mais útil para compreender a natureza e a substância do arrazoado de normas que dará corpo a um Direito da Proteção de Dados Pessoais (2.2.) identificando formas específicas de regulação (2.2.1), bem como uma abordagem baseada no risco (2.2.2.).

2.1. Direito Público ou Direito Privado?

As "situações da vida são (...) cada vez mais complexas e não se deixam capturar pelas jaulas herméticas nas quais os juristas pretendem aprisioná-las, separando-as entre públicas e privadas. Não raras vezes, as situações jurídicas comungam elementos que carecem de uma aplicação de normas de Direito Privado e de outros que antes exigem a intervenção do Direito Público"[49]. As situações jurídicas no âmbito do tratamento de dados pessoais exemplificam esta observação de M. PRATA ROQUE: por um lado, não "encaixam" na linguagem e nos modelos do Direito Público ou do Direito Privado, cuja distinção, em boa verdade, sempre foi aproximada[50]; por outro, refletem a "equivocidade" trazida pelo DUE que parte de uma "construção própria e original do direito, que não valoriza a distinção privado-público", "utiliza critérios autónomos para definição das suas categorias" e "coloca em causa a tradicional divisão entre direito público e privado"[51]. Como sintetiza F. CALVÃO, o objeto da proteção de dados pessoais "reclama uma especialização que as disciplinas tradicionais não são capazes de oferecer"[52].

Se o ponto de partida da matéria da proteção de dados, os seus alicerces, recolhem contributos da disciplina dos Direitos Fundamentais, do Direito Constitucional e do DUE, o seu

[46] Comissão Europeia, "Uma abordagem..." cit., p. 5 e Comissão Europeia, "Proteção da..." cit, p. 2.
[47] Compare-se, por exemplo, o art. 1.º, n.º 1, da Diretiva, realçando o "direito à vida privada", com o art. 1.º. n.º 2, do RGPD, destacando o direito à proteção dos dados pessoais.
[48] Art. 20.º do RGPD.
[49] Miguel Prata ROQUE, *A Dimensão Transnacional do Direito Administrativo*, AAFDL, 2014, p. 308.
[50] Em todo o caso, há quem refira a "tendencial inesgotabilidade das teses quanto à distinção entre Direito Privado e Direito Público" (M. Prata ROQUE, A Dimensão cit., p. 309) e quem procure sumariar os critérios usados para esta distinção: a participação de um órgão de autoridade, as funções desempenhadas, o enquadramento jurídico aplicável, o domínio de uma autoridade pública e o interesse prosseguido (Simon WHITAKER, "Consumer Law and the distinction between public law and private law", *The Public Law/Private Law Divide – Une entente assez cordiale*, Mark FREEDLAND, e Jean-Bernard AUBY (eds.), Hart Publishing, 2006, p. 247). Certo é que o paradigma clássico da distinção taxativa e terminante entre Direito Público e Direito Privado, como dois mundos separados, segundo uma lógica de oposição, encontra-se ultrapassado, v. P. GONÇALVES, Entidades Privadas cit., p. 271 e ss..
[51] Dulce LOPES, *Eficácia, Reconhecimento e Execução de Atos Administrativos Estrangeiros,* Policopiado, 2015, p. 118 e ss..
[52] Filipa CALVÃO, *Direito da Proteção de Dados Pessoais,* Universidade Católica, 2018, p. 32.

núcleo central será de natureza juspublicista[53]. Em todo o caso, além dos elementos de Direito Administrativo mais evidentes, como as normas que regulam a organização e o funcionamento das autoridades de controlo, conferindo-lhes incumbências de fiscalização e supervisão (art. 51.º e ss.), acham-se também neste regime elementos de Direito Privado, como o direito de indemnização (art. 82.º do RGPD) ou o contrato com o subcontratante (art. 28.º do RGPD) e, ainda, de Direito Processual Civil e Administrativo, como as regras do acesso dos titulares dos dados aos tribunais (art. 78.º e ss. do RGPD).

Não sendo possível isolar cada um destes elementos e erguer uma separação imaginária para efeitos de classificação deste regime, tem-se entendido que o mesmo congrega entrelaçamentos entre os vários ramos do direito, reunindo disposições e institutos dos mesmos cuja identificação dependerá do caso concreto[54]. Este regime é, por isso, um exemplo do "fenómeno da interconexão, sobreposição ou mistura de normas de Direito Público e normas de Direito Privado" [55]. É que mesmo admitindo uma predominância do Direito Público, este não basta para compreender todas as questões jurídicas aí abordadas[56].

Em suma, este bloco normativo encontra-se, então, numa área de confluência, numa no *man's land*[57], caraterizando-se pela sua interdisciplinaridade ao integrar normas de vários ramos do Direito. Donde tão oportunos os apelos à sua "emancipação" científica[58].

2.2. A proteção de dados pessoais no contexto da "regulação"

Uma perspetiva mais proveitosa para enquadrar o regime estudado encontra-se no conceito de "regulação". Para P. GONÇALVES a regulação é, genericamente, "um sistema de influenciação, de orientação e de controlo de processos e de comportamentos ou condutas de pessoas; esse sistema pode revelar-se de uma forma positiva (na feição de comandos, diretrizes ou recomendações) ou de uma forma negativa (na veste de proibições, limitações ou advertências) e utiliza, no seu *instrumentarium*, a edição de normas, bem como a adoção de medidas de implementação e de reação à infração do que aquelas normas estabelecem"[59].

Por um lado, o desenvolvimento diferenciado deste tipo de normatividade deve-se a um conjunto de motivos entre os quais destaco "os riscos apresentados por novos produtos e por

[53] *Idem*, p. 33.
[54] Christopher KUNER, "Data Protection Law and International Jurisdiction on the Internet (Part 1)", *International Journal of Law and Information Technology*, vol. 18, n.º 2, 2010, p. 176 e ss.. Em sentido próximo, v. Jon BING, "Data Protection, Jurisdiction and the Choice of Law", *Privacy Law & Policy Reporter,* n.º 92, 1999, disponível em http://www.uio.no/studier/emner/jus/jus/JUR5620/v08/undervisningsmateriale/Data%20Protection,%20jurisdiction%20and%20the%20choice%20of%20law.rtf, consultado no dia 30 de setembro de 2018.
[55] Pedro GONÇALVES, *Entidades Privadas com Poderes Públicos,* Almedina, 2005, p. 279.
[56] F. CALVÃO, Direito cit., p. 33.
[57] Frequente em domínios nos quais há uma prevalência de um dos ramos do direito, em termos de métodos e meios de ação que, todavia, devem ser compaginados com imperativos do outro, v. Pierre OMMESLAGHE, "Le Droit Public Existe-t-il?", *Revue de la faculté de droit et de criminologie de l'ULB*, n.º 33, 2006, p. 62.
[58] F. CALVÃO, Direito cit., p. 33.
[59] Pedro GONÇALVES, "Regulação Administrativa e Contrato", *Estudos em Homenagem ao Prof. Doutor Sérvulo Correia*, vol. II, Coimbra Editora, 2010, p. 987 e ss.. Uma análise mais recente do conceito de regulação é da autoria de Raquel CASTRO, *Constituição, Lei e Regulação dos Media*, Almedina, 2016, p. 31 e ss..

novas tecnologias"[60]. Por outro lado, compreende-se à luz de um "Estado Regulador" ou "Estado-estratega", hipótese aplicável à UE[61], que prossegue uma intervenção externa (heterorregulação) sobre atividades privadas de natureza económica, comercial e financeira tendo em vista "uma proteção ótima do 'interesse público' através da imposição de limitações ao exercício da iniciativa privada"[62]. Essa intervenção define as condições normativas de funcionamento das atividades reguladas, no cumprimento de uma "função de orientação de sistema" e, além disso, prescreve um controlo da observância de tais condições e uma punição das infrações[63]. Ou seja, a "atuação reguladora" visa conformar, dirigir, orientar, sancionar, disciplinar ou simplesmente controlar a atividade regulada[64].

O *telos* da regulação é a realização de objetivos públicos e finalidades identificadas em sede político-legislativa para promover o bem-estar social. A atuação reguladora prossegue um interesse público relacionado com objetivos sociais como a proteção dos indivíduos, defesa dos interesses ambientais, entre outros[65] – regulação social – ou estritamente económicos – regulação económica[66]. Para tanto, a iniciativa privada influenciada pela atuação reguladora não é configurada como um direito fundamental absoluto: o interesse público na prossecução e garantia de outros direitos fundamentais com aquela conflituantes pode "justificar um mero condicionamento ou até mesmo uma restrição da amplitude máxima do 'direito de iniciativa privada', sem que tal implique uma violação do parâmetro normativo constitucional"[67].

As formas de regulação desdobram-se, quanto à origem, em "regulação de origem ou proveniência privada" e "regulação de origem ou proveniência pública" [68]. Esta é um produto do poder público (estadual ou supranacional), ora provindo de "instâncias integradas na

[60] Eduardo Paz Ferreira e Luís Morais, "A Regulação sectorial da economia – introdução e perspetiva geral", E. Paz Ferreira, L. Morais e G. Anastácio, *Regulação em Portugal: Novos Tempos, Novo Modelo?* Almedina, 2009, p. 7 e ss. e Maria C. Cardona, *Contributo para o conceito e a natureza das entidades administrativas independentes – As Autoridades Reguladoras*, Almedina, 2016, p. 664.

[61] Para alguns o protótipo de um novo Estado Regulador de nível supranacional, v. Giandomenico Majone, *La Communauté européenne: un état régulateur, Montchrestien*, 1996; Marisa Apolinário, *O Estado Regulador: o novo papel do Estado*, Almedina, 2016, p. 242. Em estudos comparativos com os EUA a UE emerge como um "hiper-regulador", tendo mais apetência para aplicar soluções normativas "intervencionistas", v. Jonathan Wiener et alii (eds.), *The Reality of Precaution: Comparing Risk Regulation in the United States and Europe*, Routledge, 2010 e David Vogel, *The Politics of Precaution. Regulating Health, Safety, and Environmental Risks in Europe and the United States*, Princeton University Press, 2010.

[62] M. Prata Roque, A Dimensão cit., p. 721.

[63] Pedro Gonçalves, "Direito Administrativo da Regulação", *Regulação, Electricidade e Telecomunicações,* Coimbra Editora, 2008, p. 15, considerando o mercado como um "sistema".

[64] *Ibidem*.

[65] Busca determinados equilíbrios entre valores de mercado e outros valores correspondentes a interesses públicos, como a salvaguarda do pluralismo da informação ou outros interesses sociais de "primordial importância que transcendem, de algum modo, as puras condições de economicidade das atividades empresariais" v. Eduardo Paz Ferreira e Luís Morais, "A Regulação sectorial da economia – introdução e perspetiva geral", E. Paz Ferreira, L. Morais e G. Anastácio, *Regulação em Portugal: Novos Tempos, Novo Modelo?* Almedina, 2009, p. 23. Uma distinção aproximada é a de Vital Moreira, v. *Auto-Regulação Profissional e Administração Pública*, Almedina, 1997, p. 39 e ss..

[66] Orientada para a promoção de valores de mercado e de abertura de determinados setores económicos à concorrência, v. E. Paz Ferreira e L. Morais, "A Regulação sectorial..." cit., p. 23. Para P. Gonçalves, neste caso, a "satisfação do interesse público alcança-se, por forma indireta ou mediata, através do "correto desenvolvimento" das relações económicas e jurídicas (privadas) que se processam entre os vários atores do mercado, designadamente entre as empresas e os consumidores", v. P. Gonçalves, "Direito Administrativo da ..." cit., p. 66

[67] M. Prata Roque, A Dimensão cit., p. 720 e 721.

[68] Sem prejuízo de outros tipos de regulação de origem privada, que remeto para adiante, o instrumento mais conhecido é o contrato ou, *mutatis mutandis*, o negócio jurídico unilateral, cuja juridicidade nele expressa é desejada e produzida pelos próprios sujeitos da regulação v. P. Gonçalves, "Regulação Administrativa...", cit., p. 5.

Administração Pública", associadas à execução de uma função administrativa de regulação[69], ora de outros centros de criação de regulação pública como o poder legislativo, correspondendo a atos legislativos[70]. Quanto aos destinatários, a regulação setorial – "atinge setores determinados da economia, pelo que regulados são apenas os operadores económicos que atuam nos setores atingidos (v. g. energia, comunicações, banca)"[71] – distancia-se da regulação transversal, "aplicável à generalidade dos agentes económicos"[72], cujo caso paradigmático é a regulação da concorrência.

Mais do que caber (ou não) nas "jaulas herméticas" do Direito Público e/ou Direito Privado o regime de que me ocupo compreende-se melhor no quadro de uma atuação reguladora da UE[73]. Carateriza-se, então, como:

> (i) Regulação pública, no sentido em que é fruto do poder legislativo e exprime-se enquanto regulação administrativa nos atos praticados pelas autoridades de controlo, sejam ordens, proibições, punições, avisos, recomendações, entre outros[74].
>
> (ii) Intervenção externa nas atividades de tratamento de dados pessoais realizadas pelos utilizadores de dados pessoais, definindo as condições das mesmas, e conformando-as com imposições sujeitas a fiscalização e punição por desrespeito. Como explica F. CALVÃO: "no que aos tratamentos de dados pessoais diz respeito, a função do Estado não se pode resumir simplesmente ao acompanhamento sucessivo das atividades privadas (ou públicas), quando das mesmas possa resultar a afetação de direitos, liberdades e garantias dos membros da comunidade estatal. Isto porque, ao contrário de outras atividades, que são livres (porventura só agora desreguladas), por o seu desenvolvimento não implicar risco ou ameaça de direitos e de interesses privados e públicos, as operações que incidam sobre dados pessoais, qualquer que seja a sua natureza, não são, não podem ser livres. Falamos de atividades que são suscetíveis de ter impacto na liberdade, na privacidade, na autodeterminação ou na identidade das pessoas. E um tal impacto e um tal risco de lesão de dimensões fundamentais da dignidade da pessoa humana não podem ser ignorados, muito menos incentivados. É esta a razão por que na União Europeia não se abandona a regulação pública dos tratamentos de dados pessoais, definindo-se no plano normativo condições ou requisitos para a sua realização. E por isso a passagem do foco da função administrativa para o controlo sucessivo

[69] A "regulação" pode ser entendida enquanto missão da qual, no terreno, se ocupam as "entidades reguladoras" na sua atividade operacional, através do exercício de poderes sancionatórios, de supervisão e de regulamentação, v. P. GONÇALVES, "Direito Administrativo da...", cit., p. 20.
[70] P. GONÇALVES, "Regulação Administrativa..." cit., p. 5.
[71] *Idem*, p. 16.
[72] *Idem*, p. 17.
[73] Luiz COSTA, "Privacy and the precautionary principle", *Computer Law & Security Review*, n.º 28, 2012, p.14 e Orla LYNSKEY, *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015, p. 76.
[74] Art. 58.º, n.º 1 e 2 do RGPD.

não reflete uma conceção de que o tratamento de dados pessoais é livre, quanto ao se da sua realização, e que o controlo se limite apenas ao como da atividade"[75].

(iii) Acresce que, dado que o tratamento de dados pessoais é uma atividade que perpassa a maioria dos agentes económicos e o próprio setor público, considero tratar-se de regulação horizontal.

(iv) Por fim, reúne elementos da regulação de natureza económica e social[76].

Em relação aos primeiros, veja-se, desde logo, o potencial de afirmação e estruturação do mercado interno da UE, uma das dimensões que identifiquei. Adicionalmente, entre os objetivos da reforma que culminou com o RGPD encontra-se a pretensão de estimular a confiança do titular dos dados pessoais enquanto consumidor da economia digital[77], uma premissa para o sucesso do Mercado Único Digital que consta das prioridades da UE para os próximos anos[78]. É este binómio antitético, por um lado, incentivar o desenvolvimento tecnológico e a digitalização da economia europeia e, por outro, precaver os riscos que esse processo coloca para os titulares dos dados pessoais, que orienta este regime[79].

Por fim, depois do que já foi dito, uma componente social é clara: prevenir os riscos para o titular dos dados pessoais provocados pelo tratamento dos seus dados pessoais [80]. A regulação prossegue interesses sociais de "primordial importância que transcendem, de algum modo, as puras condições de economicidade das atividades empresariais" [81]. No âmbito destes interesses sociais caberá a dimensão jusfundamental deste regime.

2.2.1. Manifestações de "co-regulação" e de "auto-regulação publicamente regulada"

No contexto da regulação de novas tecnologias e, em especial, do ciberespaço, destaca-se o conceito de "co-regulação" espelhando uma interação entre a lei (*hard law*) e os outros modos de intervenção (*soft la*[w]). Funda-se no reconhecimento da importância de conciliar a dinâmica da regulação pública com diferentes modos de regulação privada, individual, comunitária,

[75] Filipa CALVÃO, "O modelo de supervisão de tratamento de dados pessoais na União Europeia: da atual Diretiva ao futuro Regulamento", *Fórum de Proteção de Dados*, n.º 1, julho de 2015, p. 40, disponível em https://www.cnpd.pt/bin/revistaforum/forum2015_1/index.html#40, consultado no dia 30 de setembro de 2018.
[76] O. LYNSKEY, *The Foundations of* cit., p. 9.
[77] Atente-se na redação dos considerandos 6 e 7 do RGPD a respeito da "rápida evolução tecnológica" e da "globalização" impondo "um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas".
[78] Comissão Europeia, "Mercado Único Digital para a Europa: Comissão Europeia define 16 iniciativas para a sua concretização", 6 de maio de 2015, disponível em http://europa.eu/rapid/press-release_IP-15-4919_pt.htm, consultado no dia 30 de setembro de 2018. A 12.ª iniciativa ali enunciada é a revisão da Diretiva 95/46.
[79] Rolf WEBER, "Transnational Data Privacy in the EU Digital Single Market", Dan SVANTESSON e Dariusz KLOZA (eds.), *Trans-atlantic data privacy as a challenge for democracy*, Intersentia, 2017, p. 5 e ss..
[80] O. LYNSKEY, The Foundations of cit., p. 77.
[81] E. Paz FERREIRA e L. MORAIS, "A Regulação sectorial...", cit., p. 23 e O. LYNSKEY, The Foundations of cit., p. 78.

económica e técnica[82]. Como observa A. PEREIRA: "uma coisa é deixar tudo à auto-regulação, outra bem diferente é defender a intervenção do direito estadual quando essa auto-regulação não seja possível ou gere resultados contrários aos princípios fundamentais da ordem jurídica"[83].

Paralelamente, tem-se falado de uma postura do poder público, estadual e supraestadual, que, em vez de atuar diretamente, se mostra aberto a instrumentos de ativação do "potencial endógeno da sociedade" e do "património de conhecimentos, criatividade e da capacidade dos atores privados para resolver problemas"[84]. Certos domínios são permeados por uma estratégia de reforço da responsabilidade dos privados, no âmbito da sua esfera de atuação, reposicionando o seu papel na realização do bem comum, dando azo a uma nova forma regulatória: a "auto-regulação privada publicamente regulada" ou "provocada, ativada ou induzida" pelo poder público[85]. Este conceito constitui um *tertium genus* da "ação privada desregulada" e da "direção e planificação do Estado", ou seja, a sua essência encontra-se na "associação ou combinação ou mistura entre a mera ação privada e a regulação pública ou estadual, remetendo-nos imediatamente para a ideia de Estado regulador"[86]. Há, por isso, uma continuidade entre a ação privada e a ação pública espelhada na complementaridade entre ambas[87].

Creio que o legislador da UE, no RGPD, terá seguido esta estratégia. Desde logo, entre os seus propósitos encontra-se o incentivo das "iniciativas auto-reguladoras" e dos "regimes de certificação"[88] o que leva alguns autores a registar "uma mudança significativa de regulação tipo comando-e-controlo para a inclusão de ferramentas de co-regulação na legislação de proteção de dados pessoais"[89] ou o surgimento de "um sistema de auto-regulação híbrido com arranjos públicos" [90].

[82] A regulação privada, neste sentido, tem origem em *non state actors* e baseia-se em esquemas de soft law e não em mecanismos de direito privado, como o contrato. Cfr. Lokke MOEREL, "Export of the Rule of Law: Corporate Self-Regulation of Global Data Transfers", Sam MULLER et alii, *Law of the Future Series,* n.º 1, 2012, p. 353; Maria Eduarda GONÇALVES, *Direito da Informação – Novos Direitos e Formas de Regulação na Sociedade da Informação,* 2ª ed., Almedina, 2003, p. 146 e ss.; Thibault VERBIEST e Etienne WÉRY, *Le Droit de L'Internet et de la Société de l'Information*, Larcier, 2001, p. 523.
[83] Alexandre Dias PEREIRA, *Direitos de Autor e Liberdade de Informação,* Almedina, 2008, p. 329.
[84] P. GONÇALVES, Entidades Privadas com cit., p. 14.
[85] P. GONÇALVES descreve um "novo cenário do Estado ativador" em que os privados assumem ou são convocados para desempenhar um novo papel, que partilham com o Estado, para realizar o interesse público: "Está aqui suposto, sim, o particular no seu estatuto de cidadão comprometido, empenhado e socialmente responsável (o "citoyen" e não o "bourgeois"), que procura e aceita contribuir para a realização do bem comum", podendo ser "induzido" ou obrigado a "assumir as suas responsabilidades próprias, quer na defesa dos seus direitos e interesses próprios, quer na proteção de interesses da coletividade", v. P. GONÇALVES, Entidades Privadas com cit., p. 15, 151, 161.
[86] *Idem*, p. 171.
[87] D. LOPES, Eficácia cit., p. 124.
[88] Comissão Europeia, "Uma abordagem..." cit., p. 13.
[89] Alberto GÓMEZ, "Los códigos de conducta en el reglamento general de protección de datos", J. Piñar MAÑAS et alii (coord.), *Reglamento General De Protección De Datos. Hacia um nuevo modelo europeo de privacidade,* Reus, p. 389 e ss.; Carlos SÁNCHEZ e Miguel GAYO, "Certificación en protección de datos personales", J. Piñar MAÑAS et alii (coord.), *Reglamento General De Protección De Datos. Hacia um nuevo modelo europeo de privacidade,* Reus, p. 413 e ss.; Irene KAMARA, "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'", *European Journal of Law and Technology*, vol. 8, n.º 1, 2017.
[90] L. MOEREL, "Export of the …" cit., p. 329 e ss..

Com efeito, os indícios da "auto-regulação privada publicamente regulada" e de "co-regulação" sobressaem no reconhecimento de efeitos jurídicos aos códigos de conduta destinados a "contribuir para a correta aplicação" da lei[91] e a procedimentos de certificação voluntária, selos e marcas de proteção de dados "para efeitos de comprovação da conformidade das operações de tratamento"[92].

Quanto à função destes instrumentos, visam, na perspetiva do titular dos dados pessoais, "reforçar a transparência" na medida em que lhe permitem avaliar rapidamente o nível de proteção proporcionado pelos produtos e serviços em causa e, na perspetiva dos utilizadores de dados pessoais, facilitam o cumprimento deste regime e adquirem relevo no momento da apreciação da respetiva responsabilidade[93]. Os artigos 24.º, n.º 3, 28.º, n.º 5, e o considerando 81 do RGPD determinam que a adesão àqueles instrumentos poderá indiciar a conformidade dos tratamentos de dados realizados. Do mesmo modo, nos termos do considerando 77, os códigos de conduta e as certificações aprovadas dão orientações sobre a execução de medidas e políticas adequadas e para a comprovação de conformidade com o RGPD. Por outro lado, de acordo com o art. 83.º, n.º 2, al. j), o cumprimento destes esquemas constitui um fator de mitigação na aplicação de coimas pela autoridade de controlo como, aliás, sucedeu no passado[94].

Além destas normas, o art. 21.º, n.º 5, dispõe que o direito de objeção por meios automatizados será exercido "utilizando especificações técnicas"; já os artigos 24.º, 25.º e 32.º impõem a adoção de "medidas técnicas e organizativas adequadas" [95]. Anteriormente, em 2015, a Comissão Europeia invocando, *inter alia*, o art. 8.º da CDFUE e a Diretiva, adotou uma Decisão de Implementação sobre a *standardização* no campo da política de proteção de dados e segurança e endereçou à *European Standardisation Organisation* um pedido de colaboração reconhecendo a importância deste tipo de iniciativas como complemento da sua ação regulatória[96]. A remissão para "normas técnicas" reflete a constatação de que a proteção de dados pessoais não depende apenas de soluções estritamente jurídicas que exigem ser complementadas por meios tecnológicos e pelas "Ciências das Tecnologias"[97].

Contudo, noto que o RGPD não prevê um esquema de "auto-regulação pura" ou de "regulação privada desregulada" em cujo âmbito são prestados, livremente e numa lógica de mercado,

[91] Art. 40.º do RGPD.
[92] Art. 42.º do RGPD. O art. 27.º da Diretiva 95/46 remetia para os Estados-Membros e para a Comissão Europeia a "promoção e elaboração de códigos de conduta" para facilitar o cumprimento das normas ali prescritas tendo em atenção as "caraterísticas dos diferentes setores".
[93] Considerando 100 do RGPD e Comissão Europeia, "Uma abordagem..." cit., p. 14.
[94] Kuan HON, *Data Localization Laws and Policy. The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens*, Edward Elgar Publishing, 2017, p. 211. Algumas decisões das autoridades de controlo tomaram em conta certificações de segurança standard da indústria, obtidas pela Azure (Suécia), pela Google Appps (Noruega) e pela Moss (Noruega). Por seu turno, o Grupo do Artigo 29 (G29) considerou que a "verificação ou certificação independente por um terceiro reputado pode ser uma forma credível" de demonstração de conformidade, v. G29, "Parecer 05/2012 relativo a computação em nuvem", de 1 de julho de 2012, p. 22 e 27.
[95] Eric LACHAUD, "The General Data Protection Regulation and the rise of certification as a regulatory instrument", *Computer Law & Security Review*, vol. 34, n.º 2, 2018, p. 244 e ss..
[96] Disponível em http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=refSearch.search#, consultado no dia 30 de setembro de 2018. Desenvolvendo estes instrumentos, v. I. KAMARA, "Co-regulation in EU..." cit., p. 14 e ss..
[97] F. CALVÃO, Direito cit., p. 31 e Jane WINN, "Technical standards as data protection regulation", Serge GUTWIRTH *et alii, Reinventing Data Protection?* Springer, 2009, p. 207.

serviços de certificação. O que se pretende criar é um sistema de regulação (ainda) público na medida em que é organizado pela UE, pelas autoridades de controlo ou por uma entidade privada investida da gestão do mesmo por um ato de delegação[98]. Esta opção foi motivada pelas lições de outros domínios, como o da certificação de produtos, sugerindo que a ausência de intervenção pública conduz a um nivelamento por baixo porquanto a concorrência entre fornecedores de serviços de certificação pode levar a uma redução dos preços e a uma certa flexibilidade ou relaxamento dos procedimentos[99].

Nesse sentido, o art. 43.º, n.º 9, do RGPD, remete para a Comissão Europeia a adoção de atos de execução "estabelecendo normas técnicas para os procedimentos de certificação e os selos e marcas em matéria de proteção de dados, e regras para promover e reconhecer esses procedimentos de certificação, selos e marcas"[100]. Do mesmo modo, segundo o art. 40.º, n.º 5, a produção de efeitos dos códigos de conduta depende de um processo de apreciação da sua conformidade com o interesse público a cargo da autoridade de controlo. Por outro lado, ainda que a supervisão do seu cumprimento possa ser efetuada por um organismo distinto da autoridade de controlo, tal não prejudica as competências desta que, aliás, o acredita[101]. Em sentido próximo, a competência para emitir a certificação é partilhada entre a autoridade de controlo e os organismos de certificação com base nos critérios aprovados pela primeira ou pelo Comité Europeu de Proteção de Dados Pessoais[102]. Enfim, o recurso a novos meios de regulação não aniquila uma intervenção pública que visa enquadrar e definir as condições jurídicas – materiais, formais ou organizativas – de desenvolvimento da auto-regulação privada aplicável aos tratamentos de dados pessoais.

Por conseguinte, a proteção de dados pessoais aproxima-se de um rumo, notado pela doutrina, de transformação das atuações administrativas, em relação a atividades económicas e direitos fundamentais, em intervenções meramente "certificativas ou declarativas e não autorizativas", acompanhadas pela substituição de atos prévios autorizativos que atestará "a menor intervenção pública na economia e a expansão da iniciativa económica" [103].

Esta solução simplifica a atuação administrativa (que deixa de ser prévia e autorizativa) e agiliza as atuações dos privados, mas impõe-lhes a assunção de responsabilidade[104]. Daí a centralidade do princípio da responsabilidade (art. 5.º, n.º 2 e 24.º do RGPD), um indicador do novo papel dos responsáveis pelo tratamento dados pessoais que vem descentralizar a proteção dos direitos fundamentais, ativar a quota de responsabilidade daqueles e deslocalizar a decisão sobre os riscos desses tratamentos. É desses riscos que cuido de seguida.

[98] Sobre estes sistemas v. P. GONÇALVES, Entidades Privadas cit., p. 212.
[99] G29, "Parecer 3/2010 sobre o princípio da responsabilidade", 13 de julho de 2010, p. 19.
[100] Nos termos do procedimento previsto no art. 93.º, n.º 2 do RGPD.
[101] Art. 41.º, n.º 1 e 2 do RGPD.
[102] Estes organismos são entidades oficialmente habilitadas, reconhecidas ou acreditadas, que prestam serviços privados de certificação sem exercerem funções ou poderes públicos mas antes atividades privadas que, por terem relevância pública, ficam submetidas a regulação estadual, v. P. GONÇALVES, Entidades Privadas cit., p. 213 e artigos 42.º, n.º 5 e 43.º do RGPD. O organismo nacional de acreditação é designado nos termos do Regulamento 765/2008 do PE e do Conselho, em conformidade coma norma EN-ISSO/IEC 17065/2012 e com os requisitos adicionais estabelecidos pela autoridade de controlo competente, v. artigos 43.º, n.º 1, al. b), 42.º, n.º 5 e 63.º do RGPD.
[103] D. LOPES, Eficácia cit., p. 268.
[104] *Ibidem*.

2.2.2. Uma abordagem baseada no risco

Já fui referindo os riscos dos novos tratamentos de dados pessoais surgidos com o desenvolvimento tecnológico. Mas, concretamente, que riscos são esses? A resposta a esta pergunta, lógica e cronologicamente, pode ser antecedida pela resposta a outra: será que as atividades que implicam o tratamento de dados pessoais se enquadram na chamada regulação preventiva[105]? Ou seja, os tratamentos de dados pessoais são perspetivados pelo legislador enquanto atividade causadora de "risco" que convoca uma tutela antecipada apesar da incerteza quanto à consumação de danos e à verificação de uma lesão no titular dos dados? Parece que sim[106].

Em primeiro lugar, nas fontes internacionais deste regime e na legislação dos Estados-Membros que o antecedeu, a doutrina recolheu evidências que suportam esta resposta positiva[107]. Em segundo lugar, olhando para a estrutura da relação jusfundamental no âmbito dos tratamentos de dados pessoais, esta compõe-se, *inter alia*, por um "causador de riscos" (o responsável pelo tratamento ou o subcontratante) a um bem jusfundamental (do titular dos dados). A proteção desse bem é concretizada através de regulação preventiva dos riscos gerados pelos tratamentos de dados pessoais, isto é, pela antecipação de danos em detrimento de raciocínios baseados na causalidade. Tipicamente, a *risk regulation*, definida como "uma interferência pública no mercado ou em processos sociais para controlar consequências potencialmente adversas", decompõe-se em três elementos[108]:

(i) Criação de padrões comportamentais (*standard-setting*) traduzida, *in casu*, na estatuição das condições para os tratamentos de dados;

[105] Christopher HOOD, Henry ROTHSTEIN e Robert BALDWIN, *The Governance of Risk: Understanding Risk Regulation Regimes*, Oxford University Press, 2004, p. 3; D. VOGEL, The Politics of Precaution cit., p. 5 e ss.; J. WIENER et alii (eds.), The Reality of Precaution cit., p. 10 e ss..

[106] O que gerou críticas oriundas, sobretudo, dos EUA, v. Lucas BERGKAMP, "The Privacy Fallacy: Adverse Effects of Europe's Data Protection in an Information-Driven Economy", *Computer Law & Security Review*, vol. 18, n.º 1, 2002, p. 41: "é notável que os Estados tenham adotado legislação sem qualquer evidência tangível de dano ou ameaça de dano, apenas com base numa vaga noção de direito fundamental e de riscos hipotéticos". Em sentido próximo, v. Neil RICHARDS, "The Dangers of Surveillance", *Harvard Law Review*, n.º 126, 2013, p. 1935 e ss.

[107] Entre os exemplos de instrumentos regulatórios, nacionais e internacionais, assentes na prevenção de riscos contam-se: (i) o pioneiro diploma do Länder de Hesse, cujo art. 1.º, n.º 2, na sua versão de 1999, como nota Lee BYGRAVE, visava "salvaguardar a estrutura constitucional do Estado (...) contra todos os riscos implicados pelo tratamento automatizado de dados", v. Lee BYGRAVE, *Data Protection Law. Approaching Its Rationale, Logic and Limits,* Wolters Kluwer, 2003, p. 5; (ii) na versão original das Diretrizes da OCDE, de 1980, o art. 2.º determinava a sua aplicação a "dados pessoais que, pela forma como são tratados (...) colocam em perigo a privacidade e as liberdades individuais". Vários autores perspetivam os regimes de proteção de dados como uma resposta aos riscos dos desenvolvimentos tecnológicos em geral, Christopher KUNER et alii, "Risk Management in Data Protection", *International Data Privacy Law*, n.º 5, 2015, p. 95 e ss.; José Piñar MAÑAS, "Introducción. Hacia un nuevo modelo europeo de protección de datos", J. Piñar MAÑAS et alii (coord.), Reglamento General cit., p. 21; L. COSTA, "Privacy and the precautionary …" cit., p. 14 e ss.; Maria E. GONÇALVES, "The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward", *Information and Communications Technology Law*, vol. 26, n.º 2, 2017, p. 90 e ss.; Maximilian von GRAFENSTEIN, *The Principle of Purpose Limitation in Data Protection Law*, Nomos, 2017, p. 79 e ss.; Miguel GAYO, "Aproximación basada en el riesgo, evaluación de impacto relative a la protección de datos personales y consulta previa a la autoridad de control", J. Piñar MAÑAS et alii (coord.), Reglamento General cit., p. 351 e ss.; Raphael GELLERT, "Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative", *International Data Privacy Law*, vol. 5, n.º 1, 2015, p. 3 e ss. e, do mesmo autor, "We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-based Approaches to Data Protection", *European Data Protection Law Review*, n.º 4, 2016, p. 481 e ss.; Viktor MAYER-SCHONBERGER, "Generational Development of Data Protection in Europe", Philip AGRE e Marc ROTENBERG (eds.), *Technology and Privacy: The New Landscape*, MIT Press, 1998, p. 225 e ss..

[108] C. HOOD, H. ROTHSTEIN e R. BALDWIN, The Governance cit., p. 3.

(ii) Monitorização (*monitoring*) pela autoridade de controlo; e

(iii) Modificação de comportamentos (*behaviour-modification*) visando corrigir e moldar[109] o comportamento dos utilizadores de dados pessoais na economia digital.

Em terceiro lugar, no decurso da reforma de 2012, o Grupo de Trabalho do Artigo 29 pronunciou-se favoravelmente à adoção de uma *risk-based approach* como forma de mitigar as imposições aos utilizadores de dados pessoais e delimitar a conformidade que é exigida com critérios de proporcionalidade: "o Grupo de Trabalho reconhece que algumas das normas do Regulamento podem comportar encargos em alguns responsáveis pelo tratamento que podem ser percebidos como desequilibrados e, por isso, em opiniões anteriores sugeriu que todas as obrigações sejam adaptadas ao responsável pelo tratamento e às operações de tratamento em causa. A conformidade não deve ser um exercício formalístico [*box-ticking exercise*] (…). Por conseguinte, o Grupo de Trabalho entende que os responsáveis pelo tratamento devem atuar em conformidade com a lei, mas isto pode ser feito de maneira gradual"[110]. Note-se que esta não é uma conceção nova porquanto na própria Diretiva já se podiam encontrar (tímidos) reflexos deste tipo de abordagem[111].

O que acabo de referir confirma que este regime é um exemplo de regulação preventiva. Contudo, falta identificar quais são, afinal, os riscos decorrentes do tratamento de dados pessoais. Naturalmente que não é fácil calcular o número exato dos perigos pressentidos pelo legislador quando refletiu sobre a massificação e ubiquidade dos tratamentos de dados pessoais, o aprofundamento do Mercado Único Digital e novos tratamentos como, por exemplo, a definição de perfis[112] ou a computação em nuvem[113]. Já a Diretiva não os elencava o que deu espaço para várias críticas, gerou apelos a uma solução regulatória mais focada nos danos efetivamente causados pela utilização de dados pessoais e deu o mote a propostas de

[109] Ou *un cambio de actitud* na sugestão de Luis ÁLVAREZ, "La responsabilidade del responsable", J. Piñar MAÑAS et alii (coord.), Reglamento General cit., p. 293.
[110] G29, "Statement on the role of a risk-based approach in data protection legal framework", 30 de maio de 2014, p. 2.
[111] Em relação ao nível de segurança dos dados pessoais (considerando 46 e art. 17.º, n.º 1), num reconhecimento de que certos tratamentos podem ocasionar riscos particulares e específicos para os direitos e liberdades das pessoas em causa, na exigência de controlo prévio (considerando 53 e 54 e art. 20.º), nas derrogações e restrições aos direitos do titular dos dados (art. 13.º, n.º 2 - a versão portuguesa fala em perigo, enquanto a inglesa refere o termo *risk*).
[112] Definida no art. 4.º, n.º 4, como "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos 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".
[113] Atilla KISS e Gergely SZOKE, "Evolution or revolution? Steps forward to a new generation of data protection regulation", Serge GUTWIRTH et alii (eds.), *Reforming the European Data Protection Law*, Springer, 2015, p. 313 e ss.; Catarina Sarmento e CASTRO, "A jurisprudência do Tribunal de Justiça da União Europeia, o Regulamento Geral sobre a proteção de dados pessoais e as novas perspetivas para o direito ao esquecimento na Europa", *Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos*, Vol. 1, 2016, p. 1048. A computação em nuvem é "Um tipo de computação em que são disponibilizadas, sob a forma de um serviço, capacidades escaláveis e elásticas de TI a vários clientes que utilizem tecnologias baseadas na Internet. Tipicamente, os serviços de computação em nuvem disponibilizam aplicações comuns em linha, a que os utilizadores têm acesso a partir de um navegador Web, enquanto o software e os dados são armazenados nos servidores. Neste sentido, a nuvem não é uma ilha, mas sim um conetor global das informações e utilizadores de todo o mundo", v. G29, "Parecer 1/2010 sobre os conceitos de "responsável pelo tratamento" e "subcontratante"", 16 de fevereiro de 2010, p. 10.

consagração expressa do princípio da precaução neste domínio[114]. Durante a reforma de 2012, o G29, na senda da OCDE, sugeriu uma conceção alargada de risco compreendendo qualquer efeito adverso potencial ou efetivo, incluindo efeitos sociais[115]. Na decisão *Digital Rights Ireland*, o TJ reconheceu os riscos da agregação de certos dados pessoais ("suscetíveis de permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados"[116]) e da sua retenção ("gerar no espírito das pessoas em causa (...) a sensação de que a sua vida privada é constantemente vigiada"[117]).

Finalmente, devo ainda sublinhar que no RGPD a palavra "risco" aparece para cima de 70 vezes, pelo que é difícil contestar a opção do legislador por uma abordagem assente na imprevisibilidade ou na incerteza dos efeitos dos tratamentos de dados pessoais sobre o titular dos mesmos. Mas, sobretudo, essa solução decorre diretamente, *inter alia*, das seguintes disposições[118]:

> (i) Logo no Preâmbulo o legislador regista a perceção social dos riscos, a "insegurança jurídica" e "um sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica"[119];
>
> (ii) O considerando 75 aflora o "risco para os direitos e liberdades das pessoas singulares" que "poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais", seguindo-se um elenco não exaustivo dos mesmos: a discriminação, usurpação ou roubo da identidade, perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, inversão não autorizada da pseudonimização, ou quaisquer outros prejuízos importantes de natureza económica ou social; uma privação dos direitos e liberdades do titular dos dados ou a impossibilidade de controlar os seus dados pessoais, entre outros riscos[120];
>
> (iii) De harmonia com o considerando 76, a probabilidade e a gravidade destes riscos, sendo variáveis, devem ser avaliadas, de forma objetiva, tendo em conta os seguintes elementos: a natureza, o âmbito, o contexto e as finalidades do tratamento;

[114] L. Begkamp, "The Privacy Fallacy …" cit., p. 31 e 42; L. Costa, "Privacy and the …" cit., p. 14 e ss. e O. Lynskey, The Foundations of … cit., p. 81 e ss.. Sobre este princípio na legislação de privacidade, v. Adam Thierer, "Privacy Law's Precautionary Principle Problem", *Maryland Law Review*, vol. 66, n.º 2, 2014, p. 468 e ss..
[115] G29, "Statement on the …" cit., p. 4. Sobre a OCDE, "Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data", alterada em 11 de julho de 2013, p. 24: "'Risco' é um conceito amplo, incluindo um número muito alargado de possíveis danos para o indivíduo".
[116] Acórdão do TJ, Digital Rights Ireland et alii c. Minister for Communications, Marine and Natural Resources et alii, C-293/12, 8 de abril de 2014, n.º 27.
[117] Acórdão do TJ, Digital Rights Ireland et alii c. Minister for Communications, Marine and Natural Resources et alii, C-293/12, 8 de abril de 2014, n.º 37.
[118] Aflorando medidas de mitigação dos "riscos para os titulares dos dados" como a pseudonimização (considerando 28), a propósito do consentimento de crianças e da falta de consciências dos "riscos inerentes ao tratamento" (considerando 65) e do "risco de erros" e de "potenciais riscos para os interesses e direitos do titular dos dados" como "efeitos discriminatórios" associados à definição de perfis (considerando 71),
[119] Considerando 9 do RGPD. Sobre a ideia de perceção social do risco, v. J. Pereira da Silva, Deveres cit., p. 191.
[120] Estes danos são reiterados no considerando 85 do RGPD.

(iv) A obrigação geral de responsabilidade, firmada no art. 24.º, n.º 1, é medida em função do risco dos tratamentos de dados para os direitos e liberdades das pessoas singulares, daí que em boa parte se confunda com uma obrigação de "gestão adequada dos riscos" [121];

(v) A obrigação de assegurar um "nível de segurança adequada ao risco" (art. 32.º) e de notificar a autoridade de controlo em caso de violação de dados que "seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares (art. 33.º); e

(vi) A obrigação de realizar avaliações de impacto (art. 35.º) e de notificar o titular dos dados de uma violação (art. 34.º) quando os tratamentos de dados "impliquem um elevado risco" e, portanto, ultrapassam o "risco residual", isto é, aquele que é tolerável e cuja prevenção é sempre contingente e na medida do possível[122].

Três conclusões entrelaçadas se apresentam por agora como incontornáveis: em primeiro lugar, este regime, em sintonia com o direito interno de alguns Estados-Membros[123], a opinião do G29[124] e a doutrina[125], não visa acautelar apenas danos materiais, como propôs alguma doutrina norte-americana[126]. Em segundo lugar, a inspiração preventiva deste regime formula-se do seguinte modo: havendo uma dúvida sobre a lesividade dos efeitos das atividades de tratamento de dados pessoais para o titular dos dados, a incerteza joga a favor deste impondo, aos utilizadores de dados pessoais, uma quota de responsabilidade e um conjunto de obrigações tendo em vista a "domesticação dos riscos"[127]. Em terceiro lugar, a probabilidade e a gravidade do risco que poderá resultar daquelas atividades é mensurável através de uma

[121] G29, "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 (EU) 2016/679", 4 de outubro de 2017, p. 7.
[122] "O risco residual é o perigo desqualificado, o risco cuja potencialidade lesiva já não obriga à adoção de medidas preventivas, ou simplesmente o risco que, em nome do bom senso, deve ser tolerado pela comunidade", v. Carla Amado GOMES, *Risco e Modificação do Ato Autorizativo Concretizador de Deveres de Proteção do Ambiente*, Coimbra Editora, 2007, p. 234 e 397, disponível em http://www.fd.unl.pt/docentes_docs/ma/cg_ma_17157.pdf, consultado no dia 30 de setembro de 2018; F. CALVÃO, Direito cit., p. 61, sugerindo um paralelismo com a avaliação de impacto ambiental.
[123] Em especial no Reino Unido, na decisão Google Inc. v. Vidal-Hall and others, apresentada no *Court of Appeal*, cfr. O. LYNSKEY, The Foundations of cit., p. 225. Acrescento que, a proposta inicial não aludia expressamente aos danos imateriais ou morais, tendo sido incluído posteriormente, por sugestão da Alemanha, da Eslováquia e da Suécia, v. Council of the EU, "Note from Presidency to Working Party on Information Exchange and Data Protection", 16 de dezembro de 2013, p. 540 a 544, disponível em http://www.consilium.europa.eu/en/meetings/mpo/2017/7/wp-on-information-exchange-and-data-protection-(258312)/, consultado no dia 30 de setembro de 2018.
[124] Num parecer de 1998 sobre transferências de dados pessoais afirma que "dano", na aceção da Diretiva 95/46, "inclui não apenas danos físicos e perdas financeiras, mas também qualquer prejuízo psicológico ou moral", v. G29, "Documento de Trabalho: Observações preliminares relativas ao uso de cláusulas contratuais no contexto da transferência de dados pessoais para países terceiros", 22 de abril de 1998, p. 14.
[125] O. LYNSKEY, The Foundations of cit., p. 196 e ss.: entre os danos intangíveis ou imateriais, a autora refere um sentimento de impotência do titular dos dados vis-à-vis o responsável pelo tratamento, a erosão da capacidade de autoapresentação, a inibição e o controlo de comportamentos individuais e a apreensão em relação a danos futuros.
[126] Eric GOLDMAN, "Data Mining and Attention Consumption", Katherine STRANDBURG e Daniela RAICU (eds), *Privacy and Technologies of Identity*, Springer, 2005, p. 225 e ss.; Ryan CALO, "The Boundaries of Privacy Harm", *Indiana Law Journal*, n.º 86, 2011, p. 1153.
[127] A expressão é de C. Amado GOMES, Risco e Modificação cit., p. 174.

avaliação ou classificação distinguindo-se, desde logo, o risco residual do "risco elevado"[128]. Para M. GRAFENSTEIN, esta avaliação é o principal desafio deste tipo de abordagem[129].

A doutrina tem sublinhado a vocação universalizante e a difusão do princípio da precaução para domínios que extravasam o dos riscos ambientais, em especial ao nível do DUE[130]. Contudo, não há uma referência expressa a este princípio no regime em estudo contrariamente ao que acontece noutros domínios[131]. Se é verdade que este é um princípio marcado por uma "babilónica desordem conceitual", o legislador é claro quanto à noção de risco abraçada nos considerandos 75 e 76, cuja própria probabilidade é "variável", o que implica um grau de incerteza elevado. Tal poderá indicar uma proximidade deste regime a certas conceções do princípio da precaução[132].

As consequências de uma opção regulatória assente na precaução, em domínios permeados pela incerteza e pela permanente mudança tecnológica, são várias. Desde logo, geram-se as dúvidas comuns nesta sede, como a insegurança jurídica e científica na aplicação da precaução e um indesejável "clima de suspeição crónica" que paira sobre a mesma, e convocam-se os "riscos da precaução" [133]. Para C. AMADO GOMES, este princípio pode ser entendido numa aceção radical, "equívoca e perigosa": "legitimante de uma ação pública univocamente orientada para a preservação da segurança, com sacrifício inquestionado da liberdade"[134]. A autora assume uma "resistência à precaução", afirmando, entre outros aspetos, que "suprimir sistematicamente toda e qualquer possibilidade de risco é uma atitude que privilegia a segurança de forma desproporcionada em detrimento da liberdade, amputando a dignidade humana na sua vertente mais nobre"[135]. Outros autores são menos pessimistas e procuram combater os "mitos" em torno deste princípio[136].

Em segundo lugar, faz-se sentir o decréscimo de determinabilidade da legislação por força da sua impregnação por espaços em branco assim deixados para posterior preenchimento à luz, por exemplo, de normas técnicas e de auto-regulação[137]. Como admite P. OTERO, "por

[128] Apresentando um conjunto de critérios para o definir, v. G29, "Orientações relativas à ..." cit., p. 9 e ss..
[129] M. GRAFENSTEIN, The Principle cit., p. 90.
[130] Dando nota dessa tendência para "outros domínios jusfundamentais", v. Alexandra ARAGÃO, "Aplicação nacional do princípio da precaução", *Colóquios 2011-2012,* Associação dos Magistrados da Jurisdição Administrativa e Fiscal de Portugal, 2013, p. 159 e ss. e Jorge Pereira da SILVA, *Deveres do Estado de Proteção de Direitos Fundamentais,* Universidade Católica, 2015, p. 184. Equacionando o princípio da precaução no direito da proteção de dados pessoais e sugerindo um paralelismo com o direito do ambiente, v. F. CALVÃO, Direito cit., p. 61.
[131] Alexandra ARAGÃO, "Princípio da precaução: manual de instruções", *Revista do Cedoua,* vol. 2, n.º 11, 2008, p. 16 e ss..
[132] Para J. Pereira da SILVA o princípio da prevenção distingue-se do princípio da precaução por força dos pressupostos que acionam a sua aplicação: o primeiro, mobilizado para situações de perigo e, o segundo para situações de risco. As primeiras correspondem a uma "incerteza quanto à probabilidade da lesão do bem jurídicoconstitucional ou legalmente protegido" e, as situações de risco, a "uma incerteza quanto à própria existência da probabilidade dessa lesão", v. J. Pereira da SILVA, Deveres cit., p. 170 e 181. Por seu turno, C. Amado GOMES avança que "o risco é um perigo pressentido, mas não comprovado; o perigo é um risco de altíssima probabilidade. A fronteira entre os dois é, teoricamente, a da previsibilidade, que se debate com o ineliminável obstáculo da finitude do conhecimento humano", v. C. Amado GOMES, Risco e Modificação cit., p. 226.
[133] A. ARAGÃO, "Aplicação nacional do..." cit., p. 26 e C. Amado GOMES, Risco e Modificação cit., p. 244 e ss..
[134] *Ibidem*.
[135] *Ibidem*.
[136] A. ARAGÃO, "Aplicação nacional do..." cit., p. 23 e ss.
[137] C. Amado GOMES, Risco e Modificação p. 465 e ss. e J. Pereira da SILVA, Deveres, cit., p. 563 e 573; João LOUREIRO, "Da sociedade técnica de massas à sociedade de risco – Prevenção, precaução e tecnociência: algumas questões juspublicísticas", *Estudos em homenagem ao Prof. Doutor Rogério Soares,* Coimbra Editora, 2001, p. 852. Sobre

paradoxal que possa ser (...) só uma intencional imperfeição ou incompletude de muitas das normas pode salvar as leis de uma vigência efémera em matéria de bem-estar e de prevenção de riscos"[138]. Convém ainda ter presente que a regulação dos tratamentos de dados pessoais padece do mesmo "mal" que a regulação da tecnologia em geral, descrito sob várias formas – *challenge of regulatory connection*[139], *pacing problem*[140], *Collingridge dilemma*[141] – para enunciar a rápida desatualização das soluções regulatórias em face da velocidade frenética da evolução tecnológica[142]. Daí a necessidade permanente, vertida no art. 97.º, do RGPD, de repensar e reconstruir as normas à luz dos novos tratamentos de dados pessoais e de reagir à medida dos estímulos das novas tecnologias[143]. Ou, como já foi dito, a proteção de dados pessoais é um "direito fundamental técnico" que requer atualização constante e, porventura, cada vez mais dependente, na sua efetivação, da própria tecnologia[144].

Em terceiro lugar, cabe indagar a quem compete avaliar e gerir os riscos associados ao tratamento de dados pessoais? O princípio da responsabilidade, enunciado no art. 5.º, n.º 2, do RGPD, remete esse cargo para o responsável pelo tratamento.

democracia, lei e tecnologia, v. Luís Cabral MONCADA, *Ensaio sobre a lei*, Coimbra Editora, 2002, p. 155 e, especificamente sobre o RGPD, v. Dag SCHARTUM, "Intelligible Data Protection Legislation", *Oslo Law Review*, vol. 4, n.º 1, 2017, p. 48 e ss..

[138] Paulo OTERO, *Legalidade e Administração Pública – O sentido da vinculação administrativa à juridicidade,* Almedina, 2003, p. 159.

[139] Roger BROWNSWORD, *Rights, Regulation and the Technological Revolution*, Oxford University Press, 2008 e, do mesmo autor, *Law and Technologies of the Twenty-Century: Text and materials*, Cambridge University Press, 2012.

[140] Braden ALLENBY, "Governance and Technology Systems: The Challenge of Emerging Technologies", Gary Marchant et alii (eds.), *The Growing Gap between Emerging Technologies and Legal-Ethical Oversight*, vol. 7, Springer, 2011.

[141] David COLLINGRIDGE, *The Social Control Technology*, Pinter, 1980.

[142] Fred CATE et alii, "The (Data Privacy) Law Hasn't Even Checked in When Technology Takes Off", *International Data Privacy Law*, vol. 4, n.º 3, 2014, p. 175.

[143] Aquela disposição prevê que, até ao dia 25 de maio de 2020 e, posteriormente, de quatro em quatro anos, a "Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e revisão do presente regulamento". Em sentido próximo, v. F. CALVÃO, Direito cit., p. 50 e C. Sarmento e CASTRO, "A jurisprudência..." cit., p. 1059. Sobre a necessidade de atualização das soluções adotadas em matérias caraterizadas pela incerteza e mudança permanente, v. J. LOUREIRO, "Da sociedade..." cit., p. 252; P. OTERO, Legalidade, cit., p. 293 e ss., p. 764 e ss. e p. 893 e ss..

[144] Paul DE HERT e Vagelis PAPAKONSTANTINOU, "Google Spain: Addressing Critiques and Misunderstandings One Year Later", *Maastricht Journal of European and Comparative Law*, vol. 22, n.º 4, 2015, p. 630 e Paul DE HERT, "The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents'", *Utrecht Journal of International and European Law*, n.º 31, 2015, p. 1 e ss.. Julgo que essa é uma das premissas de Alexandre Sousa PINHEIRO quando questiona se "a evolução tecnológica, e a consequente transformação das respostas jurídicas, não exige uma resposta distinta da fornecida pelo "direito à proteção de dados" nos moldes em que foi criado", v. Alexandre Sousa PINHEIRO, *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional,* policopiado, 2015, p. 63. Exemplo da transformação das respostas do direito é o conceito de *privacy by design* formalizado no art. 25.º do RGPD. Afirmando a dependência da tecnologia para garantir uma tutela efetiva dos dados pessoais, v. Woodrow HARTZOG, *Privacy's Blueprint. The Battle to Control the Design of New Technologies*, Harvard University Press, 2018.

Conclusões

Dificilmente se poderá afirmar que o Direito da Proteção de Dados Pessoais cabe, de forma rigorosa, na divisão clássica entre Direito Público/Direito Privado. Neste texto, propõe-se um ângulo de estudo para a normatividade da proteção de dados pessoais segundo o conceito de "regulação". Com efeito, de forma inequívoca, a mais recente legislação de proteção de dados pessoais, o RGPD, reflete uma intervenção legislativa sobre as atividades de tratamento de dados pessoais, do setor público e privado, tendo em vista uma proteção ótima do titular dos dados pessoais, através da imposição de condições àquelas atividades. Adicionalmente, como referi, esse tipo de intervenção prossegue com o recurso à chamada "co-regulação" ou "auto-regulação publicamente regulada" e segundo uma estratégia de prevenção de riscos cuja aplicação prática, como notado pela doutrina, será bastante desafiante.

Vídeo da apresentação

https://justicatv.com/flv/yNCzc5QZLB5XN3DqVRv82Q43b.mp4

CENTRO
DE ESTUDOS
JUDICIÁRIOS

2. Proteção de dados e emprego público

Teresa Coelho Moreira

CENTRO
DE ESTUDOS
JUDICIÁRIOS

2. PROTEÇÃO DE DADOS E EMPREGO PÚBLICO*

Teresa Coelho Moreira**

1. Introdução

1.1. O progresso da humanidade está, muitas vezes, associado ao fascínio perante a ciência e a tecnologia por originarem inovações que fazem avançar a humanidade: da roda ao microprocessador, do ábaco ao computador, da imprensa escrita à *Internet* e à *web*, *inter alia*. E, atualmente, a Inteligência Artificial[1] veio para ficar e incide sobre inúmeros aspetos da vida das pessoas em geral e dos trabalhadores em especial desde o momento de formação do contrato de trabalho[2], passando pela execução do mesmo[3] e terminando na sua cessação. A própria União Europeia num Documento de 8 de abril de 2019 sobre *Orientações Éticas para uma IA de Confiança*, estabeleceu que deveria defender-se sempre o respeito pela autonomia humana, pela transparência, pela privacidade e pela proteção de dados pessoais das pessoas, assegurando a defesa da igualdade e a proibição da discriminação, defendendo sempre a pessoa humana nas suas várias vertentes. A própria OIT[4] defendeu o mesmo quando propugna que deve fazer-se uma "uma abordagem da inteligência artificial baseada no "ser humano no comando", que garanta que decisões finais que afetem o trabalho sejam tomadas por seres humanos".

---

* Este artigo corresponde, com ligeiras alterações, ao nosso artigo intitulado "Algumas questões sobre o Regulamento Geral de Proteção de Dados e as Relações de Trabalho", *in O Regulamento Geral de Proteção de Dados e as Relações de Trabalho – Estudos APODIT VI*, (coord. MARIA DO ROSÁRIO PALMA RAMALHO e TERESA COELHO MOREIRA), AAFDL, 2020, pp. 15 e ss..

** Professora da Escola de Direito da Universidade do Minho. Membro da Direção da APODIT – Associação Portuguesa de Direito do Trabalho. Membro integrado do JusGov – Centro de Investigação em Justiça e Governação e Coordenadora do Grupo de Investigação em Direitos Humanos do mesmo.
tmoreira@direito.uminho.pt

*** Apresentação decorrente da ação de formação contínua do CEJ "Direito de Informação Administrativa e Proteção de Dados", realizada a 6 de julho de 2018.

[1] Há que referir que não existe um conceito unívoco de Inteligência Artificial, principalmente porque tem de relacionar-se com outro conceito que também é difícil de definir e que é o de inteligência humana e que a mesma coloca várias questões que ultrapassam, largamente, o âmbito deste nosso artigo mas, apenas para referir algumas, desde logo a questão da proteção e propriedade dos dados que constituem a base de trabalho para a Inteligência Artificial; ou questões relativas à responsabilidade por exemplo no caso dos carros autónomos; ou o direito à privacidade porque todos vamos deixando uma série de *pistas digitais* que permitem a comparação à entrada de determinados locais de uma cópia digitalizada e a imagem da pessoa em causa e, em especial no caso das relações de trabalho, o trabalhador encontra-se, por esta via, amplamente *radiografado* e informações colocadas *online* podem perdurar no ciberespaço por muito tempo, correndo o risco de ficarem completamente desatualizadas e com a inerente descontextualização dos dados. De notar, contudo, que o conceito está relacionado com o comportamento que uma máquina teria e que seria chamado inteligente se fosse feito por humanos e já em 1950, ALAN TURING questionou sobre se as máquinas poderiam pensar.

[2] Através de novas formas de contratação *online*, *inter alia*, com o recurso a um novo tipo de entrevistas, ou de recurso a plataformas digitais de emprego.

[3] Através de, *inter alia*, um novo tipo de formação ao longo da vida, de um novo controlo, o controlo eletrónico/digital, um novo tempo de trabalho, ou de um novo tipo de Direito Coletivo.

[4] *Trabalhar para um Futuro Melhor*, Genebra, 2019.

1.2. Por outro lado, o dom da ubiquidade é apanágio divino. Porém, atualmente, a *Internet* granjeou esse atributo, colocando cada vez mais incisivamente questões delicadas à privacidade. E a informática entronizou-se como um verdadeiro símbolo da nossa cultura a tal ponto de se denominar a sociedade moderna como *sociedade informática ou sociedade de informação* e como a era da *Big Data*[5], que coloca novos desafios à privacidade das pessoas em geral, e dos trabalhadores em especial, parecendo dar-se prevalência ao valor económico relacionado com os dados pessoais e não ao seu valor jurídico. O computador transformou a economia, a sociedade, a cultura e, inclusive, o ser humano. Esta nova realidade não poderia passar à margem do Direito do trabalho, de maneira tal que hoje é corrente a expressão *nudez tecnológica* do trabalhador, na medida em que existe uma automatização de dados sobre o trabalhador que, muitas vezes, incide sobre aspetos que fazem parte da sua privacidade e que, por isso, estão protegidos e tutelados juridicamente. Estes dados tornaram-se uma nova forma de economia e com um alto valor económico e social, sendo que a questão essencial que se coloca agora já não é a de saber quem pode aceder aos dados pessoais das pessoas mas onde estão esses dados e quem poderá aceder a eles na medida em que, com as novas formas de comunicação, qualquer pessoa pode ser um "controlador de dados"[6].

1.3. Por outro lado, a utilização cada vez maior de novas tecnologias de informação e comunicação nos últimos anos tem aumentado exponencialmente refletindo-se no mundo do trabalho e levantando várias questões. Existe, atualmente, uma enorme quantidade de dispositivos eletrónicos, desde, *inter alia*, a videovigilância, que engloba agora todos os sensores num contexto da Internet das Coisas, a audiovigilância, a geolocalização, o controlo das comunicações eletrónicas, o controlo através das redes sociais, das mensagens instantâneas, dos dados biométricos, do reconhecimento facial, da crescente utilização da *Inteligência Artificial*, que permitem monitorizar, virtualmente, todos os aspetos da vida profissional, assim como a vida extraprofissional, e mesmo, por vezes, a vida íntima dos trabalhadores, muitas vezes através do cruzamento deste tipo de informação, bastando imaginar um sistema de videovigilância que utilize, simultaneamente, um sistema de reconhecimento facial para analisar o padrão de comportamento dos trabalhadores e punir disciplinarmente quem se desvie do padrão estabelecido[7]. Surgem novas formas de controlo relacionadas nomeadamente com a utilização de serviços *online* ou de dados de localização a partir de dispositivos inteligentes que, apesar de serem muito menos visíveis para os trabalhadores quando comparados com os meios tradicionais de controlo, não deixam de ter uma enorme capacidade de controlo. E esta aparente *invisibilidade* técnica do controlo realizado pelo empregador levanta questões relacionadas com a extensão do conhecimento real que os trabalhadores têm da mesma[8].

Há, na verdade, inúmeros desafios para a privacidade dos trabalhadores na vertente de dados pessoais na era da *Big Data*, pois a possibilidade de utilização indevida e abusiva dos mesmos é muito superior na era digital. Neste sentido, a proteção dos dados pessoais, sobretudo no

[5] OMER TENE e JULES POLONETSKY, "Privacy in the Age of Big Data: A Time for Big Decisions", *in Stand. L. Rev. Online*, vol. 64, n.º 63, 2012, p. 63, assim como JOSHUA GRUENSPECHT, "Reasonable Grand Jury Subpoenas: Asking for Information in the Age of Big Data", *in Harvard Journal of Law Technology*, vol. 24, n.º 2, 2011, pp. 544-545.
[6] Cf. JANE YAKOWITZ, ""Tragedy of the Data Commons", *in Harvard Journal of Law Technology*, vol. 25, n.º 1, 2011, pp. 2-3.
[7] Veja-se o exemplo dado pelo Grupo de Trabalho do Artigo 29.º em *Opinion 2/2017 on Data Processing at Work*, de 8 de junho de 2017, p. 19.
[8] Neste sentido cf. Grupo de Trabalho do Artigo 29.º em *Opinion…*, cit., p. 4.

campo da internacionalização deve ser aprimorada e alterada. Contudo, isto não significa que não se deva ter em atenção as inúmeras vantagens da era da *Big Data*, parecendo-nos que a tensão entre proteção de dados e interesses económicos pode ser parcialmente resolvida com uma maior e melhor proteção daqueles, tornando-se a mesma até uma vantagem competitiva[9].

1.4. Atendendo aos perigos inerentes a esta situação a Comissão Europeia elaborou a 25 de janeiro de 2012 um *pacote de medidas* destinadas a alterar a regulamentação da proteção de dados pessoais numa espécie de *Revolução Copernicana*, apresentando uma Proposta de Regulamento sobre Proteção de Dados Pessoais.

E, após um longo périplo legislativo, foi aprovado o Regulamento Geral de Proteção de Dados Pessoais 2016/679, de 27 de abril que entrou em vigor no dia 25 de Maio de 2016 e previa um período transitório de dois anos para a sua total aplicação, que aconteceu a 25 de maio de 2018, devendo as organizações utilizar aquele período de tempo para se adaptarem às novas regras.

Este Regulamento traz inúmeras implicações para as relações de trabalho, quer através da clarificação de alguns conceitos, quer através do surgimento de novos direitos, quer, ainda, através do surgimento de novas figuras[10].

2. Alguns tratamentos de dados pessoais dos trabalhadores em Portugal e o Regulamento Geral de Proteção de Dados Pessoais

A relação de trabalho exige, por vezes, o tratamento de inúmeros dados pessoais dos trabalhadores, na aceção do art. 4.º, n.º 1, do Regulamento Geral de Proteção de Dados Pessoais, assim como o tratamento dos mesmos[11], na medida em que é necessária a obtenção de informação e esta é arquivada, acedida e analisada. Vários são os dados que poderão ser alvo deste tratamento, desde dados pessoais como os CV, certificados de formação, candidaturas, notas de entrevistas, assim como dados pessoais sensíveis[12], como sejam os dados biométricos, os dados de saúde, dados genéticos, ou, ainda, imagens de videovigilância, ou dados de geolocalização. É ainda possível o tratamento de dados pessoais relacionados com a informação sobre quando o trabalhador iniciou a sua jornada de trabalho e quando terminou através de *logins* informáticos - que poderão utilizar o recurso a dados biométricos -, ou de sistemas de controlo de assiduidade, que também poderão utilizar estes mesmos dados.

2.1. O art. 88.º com a epígrafe *Tratamento no contexto laboral*, é bastante importante porque permite que "Os Estados-Membros possam estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o

[9] Neste sentido *White Paper Work 4.0,* Alemanha, 2016, p. 35
[10] Para maiores desenvolvimentos *vide* TERESA COELHO MOREIRA, "Algumas Implicações Laborais do Regulamento Geral de Proteção de Dados Pessoais no Trabalho 4.0", *in Questões Laborais*, n.º 51, 2018.
[11] Art. 4.º, n.º 2, do RGPD.
[12] Cf. art. 9.º, n.º 1 do RGPD.

cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho, sendo que estas normas incluem medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho, devendo os Estados-Membros notificarem a Comissão das disposições de direito interno que adotarem nos termos do n.º 1, até 25 de maio de 2018 e, sem demora, de qualquer alteração subsequente das mesmas".

Este artigo resulta da consciencialização das inúmeras possibilidades de controlo através das novas tecnologias, assim como das diferenças em termos de proteção laboral relativamente ao tratamento de dados pessoais dos trabalhadores nos diferentes Estados-Membros.

Tendo em atenção a redação deste artigo e a ampla proteção conferida no Código do Trabalho relativamente a esta matéria consideramos muito positivo que o legislador português tenha acionado este artigo na Lei n.º 58/2019, de 8 de agosto, ao estabelecer um artigo com a epígrafe *relações laborais* - art. 28.º, em que no n.º 1, prevê que "O empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais, com as especificidades estabelecidas no presente artigo."

2.2. A noção de dados pessoais presente no art. 4.º do RGPD é mais ampla do que a anterior pois considera como dados pessoais toda a "informação relativa a uma pessoa singular identificada ou identificável", sendo 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**[13] ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Esta noção é bastante interessante e com relevante interesse prático para o Direito do trabalho e que nas empresas que trabalham na *cloud* adquire enorme importância. Também é importante porque é mais abrangente englobando os dados de localização o que significa, claramente, que a utilização dos mesmos numa relação de trabalho terá de ser considerada como um meio de vigilância à distância, e que não podem cingir-se à videovigilância ou à áudio-videovigilância, já que permitem um controlo permanente e remoto, a uma distância temporal e espacial, dos trabalhadores, sendo-lhes aplicável o previsto nos artigos 20.º e 21.º do CT, e, mais concretamente, os números 1 e 2 do art. 20.º relativo às condições de licitude da instalação deste tipo de sistemas e ao princípio da finalidade legítima.

[13] Negrito nosso.

Estas tecnologias de geolocalização têm uma enorme capacidade de controlar a localização geográfica, quer de objetos, quer de pessoas, tendo a sua mesma vindo a melhorar nos últimos anos, sobretudo se associadas à tecnologia por radiofrequência[14]. Assim, atualmente, é possível através de um dispositivo móvel equipado com sistema de GPS saber a localização de pessoas e de objetos com uma diferença de apenas 1 a 2 metros em relação à sua localização real, não apenas em locais situados no exterior de edifícios mas inclusive no interior e, por vezes, em locais extremamente íntimos. É possível, através deste meios, o controlo contínuo dos trabalhadores, não apenas durante a jornada de trabalho mas também fora desta.

Na verdade, como os dispositivos de geolocalização podem estar inseridos no *smartphone* ou no *tablet* dos trabalhadores, e estes estão indissociavelmente ligados aos seus utilizadores, inúmera informação pode ser obtida, incluindo alguma relacionada com a privacidade do trabalhador e, até, com a sua esfera mais íntima. No caso da realização de tratamento de dados de geolocalização sem conexão com a vida profissional do trabalhador, ou seja, na sua vida extraprofissional, este é vedada ao empregador. Assim, se o trabalhador tiver um veículo da empresa para uso laboral e, simultaneamente, extralaboral, a eventual legitimidade de tratamento de dados de geolocalização cinge-se à utilização profissional, já que a geolocalização não deve servir para prolongar a subordinação jurídica do trabalhador para além do limite temporal acordado. Qualquer tratamento de dados pessoais para além desta utilização será ilícita e recairá sobre o empregador o ónus de criar mecanismos que permitam um *switch off* dos dispositivos na vida privada, consoante o trabalhador esteja a trabalhar ou não. Porém, há situações em que os dispositivos de GPS estão ligados ao motor do veículo e, por isso, é impossível a utilização deste mecanismo de *swtich off*. Nestes casos, a tecnologia pode auxiliar na proteção da privacidade dos trabalhadores através do recurso à tecnologia de *privacy by design*, significando que é o próprio dispositivo técnico que cria a possibilidade de proteger a privacidade dos trabalhadores através de mecanismos para separar a utilização profissional da utilização pessoal, ficando a primeira acessível ao empregador e a outra inacessível, ainda que, em caso de furto ou roubo, por exemplo, essa informação esteja registada e possa ser utilizada pelas autoridades competentes[15].

Aliás, é o próprio Regulamento Geral que aponta para esta ideia no art. 25.º que chama a atenção para o facto de a tecnologia poder ser vista como amiga da privacidade, através da consagração da *proteção de dados desde a conceção e por defeito*, estabelecendo que "tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, **o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente**

[14] Sobre esta veja-se, para maiores desenvolvimentos, TERESA COELHO MOREIRA, "A privacidade dos trabalhadores e a utilização de tecnologias de identificação por radiofrequência", *in Estudos de Direito do Trabalho*, reimp. da 1.ª edição, Almedina, Coimbra, 2016.

[15] Para maiores desenvolvimentos *vd.* TERESA COELHO MOREIRA, "O controlo dos trabalhadores através de sistemas de geolocalização", *in Estudos de Direito do Trabalho, Volume II*, Almedina, Coimbra, 2016.

regulamento e proteja os direitos dos titulares dos dados", assim como "O responsável pelo tratamento **aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade**[16]**.** Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares".

Este princípio é crucial porque incorpora a proteção de dados pessoais em todo o ciclo da vida das tecnologias.

Já o considerando 78 do Regulamento refere que a defesa dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados pessoais exige a adoção de medidas técnicas e organizativas adequadas, a fim de assegurar o cumprimento dos requisitos do presente regulamento. Para poder comprovar a conformidade com o presente regulamento, o responsável pelo tratamento, no caso o empregador, "deverá adotar orientações internas e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a conceção e da proteção de dados por defeito".

Por outro lado, considerando que os sistemas de geolocalização são meios de vigilância à distância, não podem ser utilizados para controlar o desempenho profissional dos trabalhadores, tal como sempre foi interpretado para os meios tradicionais como a videovigilância, pois tal é vedado pelo art. 20.º, n.º 2 do CT. Os dados pessoais, mesmo que recolhidos para outras finalidades legítimas, não podem ser utilizados direta ou indiretamente para a avaliação do desempenho do trabalhador[17].

Assim, só quando existir uma finalidade legítima como a do respeito pela segurança de pessoas e bens é que poderão instalar-se estes meios. Torna-se inquestionável que o empregador deve ter a possibilidade de salvaguardar o seu património e o de terceiros, assim como o dos seus trabalhadores, perante eventuais agressões ou atentados provenientes de próprios trabalhadores ou de terceiros, impedindo ou verificando a sua realização com os instrumentos que a técnica coloca à sua disposição, e, no caso concreto, através da utilização de meios de vigilância à distância. Consideramos, contudo, que têm de ocorrer situações de razoável risco para a segurança ou um perigo concreto e não apenas uma finalidade genérica preventiva ou de segurança.

A instalação deste tipo de sistemas também pode estar justificada por várias exigências relacionadas com a natureza da própria atividade, nos termos do art. 20.º, n.º 1 do CT.

[16] Negrito nosso.
[17] Veja-se, a titulo de exemplo, que na Lei de Proteção de Dados Pessoais da Áustria, - *Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000)* - na secção III, parágrafo 12, n.º 4, 2, é proibida a gravação de imagens para controlar os trabalhadores - *eine Bildaufnahme zum Zweck der Kontrolle von Arbeitnehmern* -, assim como no n.º4, analisar dados pessoais sensíveis através das imagens obtidas - *die Auswertung von mittels Bildaufnahmen gewonnenen personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) als Auswahlkriterium*.

2.3. Outra das ideias presentes no Regulamento Geral de Proteção de Dados com enorme importância para a relação de trabalho é a definição de consentimento do titular de dados pessoais para tratamento de dados.

Na verdade, este Regulamento Geral retirou o acento tónico do consentimento como fundamento jurídico válido para o tratamento de dados pessoais quando, nos termos do considerando 43, "exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento", como é o caso, claramente, da relação de trabalho. Este considerando é muito importante porque significa que para que um tratamento de dados pessoais realizado pelo empregador seja válido terá de assentar noutros princípios que não o mero consentimento do trabalhador. E esta ideia é reforçada quer pela redação do próprio art. 4.º, ao definir que o consentimento do titular dos dados é "uma manifestação de vontade, **livre**[18], específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento", quer pelo próprio art. 7.º, sobretudo os números 1 e 4, que estabelecem, respetivamente, que "quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais", e que "ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato" [19].

Parece-nos, sem dúvida, que a noção de consentimento, entendido como uma manifestação de vontade livre, específica e informada, é um conceito de difícil concretização e de difícil preenchimento no contexto de uma relação de trabalho e, por isso, saúda-se, vivamente, a redação e a clarificação realizada no Regulamento.

Considera-se que, no âmbito laboral, o requisito do consentimento fica relegado para um segundo plano já que o trabalhador interessado se encontra numa posição de desigualdade

[18] Sublinhado nosso, sendo que este é o que falta numa relação de trabalho. As relações de trabalho são um exemplo paradigmático da existência de relações privadas desiguais não só no plano factual mas também no plano jurídico. Na verdade, no plano factual, os sujeitos contraentes – trabalhador e empregador – não dispõem da mesma liberdade no que concerne à celebração do contrato nem à estipulação de cláusulas contratuais, o que origina o aparecimento de um desequilíbrio contratual que se acentua em alturas de desemprego generalizado. No plano jurídico, a conclusão do contrato de trabalho coloca o trabalhador numa situação de subordinação face ao empregador. Assim, figurando-se o domínio económico e social de uma parte, não se pode invocar, sem mais, o princípio da liberdade contratual, para se poder escolher arbitrariamente a contraparte, ou seja, o trabalhador.

[19] É interessante notar que o Grupo de Proteção de Dados Pessoais do art. 29.º, no seu *Parecer 15/2011 sobre a definição de consentimento*, de 13 de julho de 2011, já tinha defendido que, para que o consentimento fosse válido como legitimador do tratamento de dados pessoais, teria de ser livre, considerando que "O consentimento apenas será válido se a pessoa em causa puder exercer uma verdadeira escolha e não existir nenhum risco de fraude, intimidação, coação ou consequências negativas importantes se o consentimento for recusado. Se as consequências do consentimento comprometerem a liberdade de escolha da pessoa, o consentimento não será livre. A própria diretiva prevê, no artigo 8.º, n.º 2, alínea a), que, em certos casos, a serem determinados pelos Estados-Membros, a proibição de tratamento de categorias especiais de dados pessoais não pode ser ultrapassada pelo consentimento da pessoa em causa. Um exemplo disto é o caso em que a pessoa em causa está sob a influência do responsável pelo tratamento dos dados, como no caso de um vínculo laboral. Neste exemplo, embora não necessariamente, a pessoa em causa pode encontrar-se numa situação de dependência em relação ao responsável pelo tratamento dos dados - devido à natureza da relação ou a circunstâncias especiais - e pode temer retaliações se não consentir no tratamento dos seus dados".

em relação ao responsável pelo tratamento, isto é, o empregador, desigualdade na sua necessidade de obtenção de um posto de trabalho, no caso dos candidatos a emprego, ou de manutenção do mesmo, no caso de trabalhadores. Não parece que neste tipo de relação se possa falar de um consentimento prestado livremente, principalmente quando o consentimento é requisito para a obtenção de um serviço essencial ou, no caso que aqui nos interessa, para a manutenção de um posto de trabalho, não podendo falar-se aqui de uma verdadeira liberdade de escolha[20].

Quando uma das partes está submetida ao poder contratual de outrem, não usufruindo de suficiente margem de defesa dos seus próprios interesses e de autoafirmação, o seu consentimento em relação ao contrato e aos vários termos deste não confere qualquer garantia substancial de integrar uma manifestação verdadeira de autodeterminação.

Contudo, não pode deixar de ter-se em atenção que na relação laboral torna-se necessária a recolha de numerosas informações dos trabalhadores para a correta execução do contrato de trabalho, sendo, assim, este tratamento uma consequência quase *natural* deste tipo de relações. Atendendo a tudo isto, defende-se uma inevitável evolução no sentido de colocar o pressuposto legitimador do tratamento de dados pessoais não no consentimento individual do trabalhador mas na ampliação do número de pressupostos alternativos a este consentimento. Entende-se que deve assumir importância a técnica de tipo objetivo, isto é, que assente a legitimidade do tratamento no respeito pelo princípio da finalidade e no prosseguimento de fins específicos e não de outros, colocando o acento tónico neste princípio e na ideia do tratamento ser pertinente e necessário, respeitando sempre o princípio da proporcionalidade.
Esta construção parece-nos trazer uma maior dose de garantia do ponto de vista laboral, já que, ainda que o consentimento do trabalhador tenha sido prestado[21], se o tratamento não respeitar estes princípios, isto é, se não for pertinente, nem necessário, ou não tiver uma finalidade lícita, será sempre ilícito. O carácter irrenunciável dos direitos de personalidade a isso obsta.

2.3.1. No ordenamento jurídico português, a Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica interna, do Regulamento, estabeleceu no art. 28.º, n.º 3, algumas regras relativas ao consentimento do trabalhador, mas que nos parecem não ter a melhor redação, sobretudo o n.º 3, alínea a), que preconiza "salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais: **se do tratamento resultar uma vantagem jurídica ou económica para o**

[20] O mesmo foi defendido pelo Grupo de Trabalho do art. 29.º, *Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679,* adotadas em 28/11/2017, última redação revista e adotada em 10/04/2018 p. 7, quando estabelecem que "Atendendo à dependência que resulta da relação empregador/trabalhador, é improvável que o titular dos dados possa recusar ao seu empregador o consentimento para o tratamento dos dados sem que haja medo ou risco real de consequências negativas decorrentes da recusa. É improvável que um trabalhador responda livremente ao pedido de consentimento do empregador para, por exemplo, ativar sistemas de controlo como a observação do local de trabalho através de câmaras ou preencher formulários de avaliação, sem sentir qualquer tipo de pressão para dar esse consentimento. Por conseguinte, o GT29 considera problemática a questão de os empregadores procederem ao tratamento de dados pessoais dos seus trabalhadores atuais ou futuros com base no consentimento, uma vez que é improvável que esse consentimento seja dado de livre vontade. Relativamente à maior parte deste tratamento de dados no local de trabalho, o fundamento legal não pode nem deve ser o consentimento dos trabalhadores [artigo 6.º, n.º 1, alínea a)], devido à natureza da relação entre empregador e trabalhador".
[21] Sem a verdadeira liberdade que é essencial.

trabalhador"[22]. Na verdade, retirar a necessidade de consentimento quando possa resultar uma vantagem jurídica ou económica não nos parece fazer muito sentido e afigura-se-nos ir contra o disposto no próprio Regulamento Geral já que este, no considerando 42, refere que o consentimento não é livre quando o titular de dados pessoais não possa recusar ou retirar o consentimento sem com isso ser prejudicado. O GRUPO DE PROTEÇÃO DE DADOS DO ARTIGO 29.º[23] defendeu que "o consentimento só pode ser válido se o titular dos dados puder exercer uma verdadeira escolha e **não existir qualquer risco de fraude, intimidação, coação ou consequências negativas importantes (p. ex. custos adicionais substanciais) se o consentimento for recusado. O consentimento não será dado livremente nos casos em que exista qualquer elemento de obrigatoriedade, pressão, incapacidade de exercício da livre vontade"**[24].

Defende-se, aliás, que deveria ter-se alterado a redação e colocado que "salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais: **se do tratamento não resultar uma vantagem jurídica ou económica para o trabalhador**"[25], sob pena de o preceito não fazer sentido, na nossa opinião[26].

Claro que um problema que se levanta é o de saber o que deve ser entendido por vantagem, porque o legislador não nos confere qualquer noção da mesma. Atendendo a isso defende-se que tem de ser sempre uma verdadeira vantagem, uma vantagem inequívoca, e uma vantagem considerável já que temos muitas dúvidas sobre a verdadeira liberdade do consentimento prestado por um trabalhador e, ainda mais, por um candidato. Concorda-se, por isso, com o decidido pela CNPD na Deliberação n.º 2019/494, de 3 de setembro, que decidiu desaplicar algumas normas desta Lei, nomeadamente o artigo 28.º, n.º 3, alínea a), por parecer traduzir-se "numa restrição não adequada, desnecessária e excessiva do direito fundamental à autodeterminação informacional ou à proteção dos dados enquanto direito ao controlo dos seus próprios dados, para lá do que é necessário à salvaguarda dos direitos e interesses dos trabalhadores".

[22] Negrito nosso. Ver, em sentido oposto, isto é, considerando que pode entender-se como um consentimento livre, o § 26, 2, da Bundesdatenschutzgesetz, que estabelece que "2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. **Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird** oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung hat schriftlich oder elektronisch zu erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären" – negrito nosso.

[23] *Orientações relativas ao…*, cit., p. 8.

[24] Negrito nosso.

[25] Negrito nosso. Aliás, este aspeto foi também criticado no Parecer n.º 20/2018, de 2 de maio, da Comissão Nacional de Proteção de Dados (http://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368,, p. 36), onde se pode ler que a Comissão "admite que a redação decorra de um qualquer lapso que torna, na realidade, o preceito incompreensível. Pretende-se, talvez, clarificar que o consentimento do trabalhador não releva, por regra, como condição de licitude de tratamentos de dados pessoais pelo empregador, precisamente porque a natureza não paritária da relação laboral não permite assegurar a liberdade da manifestação de vontade do trabalhador, requisito imprescindível de relevância jurídica do consentimento".

[26] Perante esta aparente desnecessidade do consentimento do trabalhador quando resultar uma vantagem jurídica ou económica para o trabalhador, este não a pode recusar? Não nos parece. Entende-se que o trabalhador tem direito a recusar essa vantagem.

2.3.2. Assim, tendo em atenção a irrelevância do consentimento, o tratamento de dados pessoais dos trabalhadores na relação de trabalho só poderá ser feito atendendo a certos princípios fundamentais que são os que já existem atualmente nos artigos 14.º a 22.º do CT mas que agora foram de certa forma clarificados e reforçados pelo Regulamento Geral de Proteção de Dados Pessoais.

Desta forma, o único fundamento que pode legitimar o tratamento de dados pessoais na relação de trabalho é a prossecução de interesses legítimos da entidade empregadora aferíveis em função do caso concreto, e nos termos do art. 6.º, n.º 1, alínea b), do RGPD, quando o tratamento for necessário para a execução do contrato de trabalho.

Assim, o empregador, antes da adoção de qualquer medida de controlo eletrónico que implica um tratamento de dados pessoais do trabalhador que, ainda mais podem ser sensíveis, tem de respeitar o princípio da finalidade. Este princípio está previsto no art. 5.º, n.º 1, alínea b), do Regulamento e significa que os dados de carácter pessoal apenas podem ser recolhidos quando existam motivos determinados, explícitos e legítimos, e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades, indicando que os dados pessoais dos trabalhadores só podem ser tratados se respeitarem estes pressupostos, sendo essencial a definição precisa destas finalidades.

Este princípio constitui o princípio verdadeiramente cardinal da proteção de dados, sendo os demais princípios função deste na medida em que os dados devem ser adequados, pertinentes e não excessivos em relação à finalidade pretendida; devem ser exatos, completos e atualizados em função da finalidade; e só devem ser conservados pelo tempo que a finalidade exige.

Assim, a finalidade pretendida pelo empregador tem de ser legítima, isto é, deve estar em conformidade com o ordenamento jurídico e ser especialmente respeitadora dos valores fundamentais.

Veja-se, por exemplo, no caso das indagações possíveis e vedadas ao empregador quer na fase de execução do contrato de trabalho, quer na fase de seleção, a redação dada ao art. 17.º, n.º 1, alínea a) e b) do CT, distinguindo os dados relativos à vida privada e saúde e estado de gravidez, só pode questionar-se quando “estas sejam estritamente necessárias e relevantes para avaliar da respetiva aptidão no que respeita à execução do contrato de trabalho” ou “salvo quando particulares exigências inerentes à natureza da atividade profissional o justifiquem”.

Também relativamente aos dados pessoais no caso de meios de vigilância à distância, artigos 20.º e 21.º do CT, o princípio da finalidade é essencial antes da instalação de qualquer destes meios pois se a regra é a sua proibição, em determinados casos poderão ser instalados desde que “tenha por finalidade a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade o justifiquem”. Apenas nestes casos poderão ser instalados.

No caso destes meios de vigilância à distância e, especificamente, na videovigilância, com as capacidades fornecidas pela análise de vídeo, é possível a um empregador monitorar as expressões faciais do trabalhador por meios automatizados, para identificar desvios de padrões de movimento predefinidos (por exemplo, contexto de fábrica) e muito mais. Isso seria desproporcional aos direitos e liberdades dos trabalhadores e, portanto, geralmente ilegal. O processamento também é suscetível de envolver o perfil, e possivelmente, a tomada automática de decisões, bastando ter em atenção o Considerando 71 da Diretiva que estabelece "O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónica ou **práticas de recrutamento eletrónico sem qualquer intervenção humana**. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para **avaliar aspetos pessoais relativos a uma pessoa singular**, em especial a análise e previsão de **aspetos relacionados com o desempenho profissional**[27], a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar", assim como o art. 22.º com a epígrafe *Decisões individuais automatizadas, incluindo definição de perfis*[28].

Neste sentido, os empregadores devem abster-se do uso de tecnologias de reconhecimento facial e sobretudo ser vedado a estes o cruzamento dos dados da videovigilância com dados biométricos e isto, infelizmente, não vem estabelecido na Lei 58/2019.

Aliás, relativamente aos dados biométricos, convém ter em atenção que o Regulamento estabelece no art. 9.º, a proibição, como regra geral do tratamento de certas categorias de dados pessoais, considerados dados sensíveis e que têm implicação direta na relação de trabalho, e que são a "origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos[29], **dados biométricos para identificar uma pessoa de forma inequívoca**[30], dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa". Não deixa de ser interessante notar a inclusão quer dos dados genéticos, quer dos dados biométricos, que não se encontravam na Diretiva 95/46/CE, apesar dos primeiros constarem da Lei 67/98, de 26 de outubro que transpôs a Diretiva.

Apesar desta proibição geral, a alínea b) do n.º 2 deste artigo permite mas apenas se "o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral", assim como a alínea h) relacionada com os serviços de medicina do trabalho, ao estabelecer que será possível "Se o tratamento for necessário para efeitos de

[27] Negrito nosso.
[28] Para maiores desenvolvimentos veja-se a Opinião do Grupo do Artigo 29.º, de 3 de outubro de 2017, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*.
[29] Relativamente a estes veja-se o art. 13.º da Lei n.º 12/2005, de 26 de janeiro, assim como LEAL AMADO, "Breve apontamento sobre a incidência da revolução genética no domínio juslaboral e a Lei n.º 12/2005, de 26 de Janeiro", *in Temas Laborais*, Coimbra Editora, Coimbra, 2005.
[30] Negrito nosso.

medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado". Contudo, neste último caso, o n.º 3 preconiza que os dados pessoais podem ser tratados se "forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes"[31].

O Código do Trabalho português regula o tratamento de dados biométricos no art. 18.º, e na Lei 58/2019, de 8 de agosto, onde o art. 28.º, n.º 6, estabelece que "o tratamento de dados biométricos dos trabalhadores só é considerado legítimo para controlo de assiduidade e para controlo de acessos às instalações do empregador". Mais uma vez, defende-se que este preceito poderia ter uma melhor redação. Apesar de este preceito ter de ser conciliado com o n.º 2 do art. 18.º do CT que preconiza que "O tratamento de dados biométricos só é permitido se os dados a utilizar forem necessários, adequados e proporcionais aos objetivos a atingir", entende-se que deveria ter outra redação. Em primeiro lugar preconiza-se que os sistemas biométricos podem ser utilizados não apenas para controlo da assiduidade, mas também da pontualidade. Em segundo lugar, considera-se que é um interesse legítimo do empregador pretender que determinados espaços da empresa sejam acessíveis apenas a alguns trabalhadores e o controlo de acesso a esses locais, se preencher todos os restantes requisitos, pode ser feito por dados biométricos. A ser assim, terá de fazer-se uma interpretação extensiva da parte do artigo da Proposta que se refere a "controlo de acessos às instalações do empregador".

Por outro lado, é possível também que o acesso a dispositivos móveis e informáticos seja feito por dados biométricos. Ora, também esta finalidade nos parece legítima. Mas não consta do art. 28.º, n.º 6. Significará que não será admissível? Não nos parece a melhor solução esta inadmissibilidade. Aliás, assemelha-se-nos que neste número, na primeira parte, o legislador restringiu em demasia o princípio da finalidade e as situações em que é possível o recurso aos dados biométricos e, por outro lado, na segunda parte, deveria ter sido mais restritivo.

Considera-se, ainda, atendendo às inúmeras possibilidades de controlo através deste tipo de dados, e na senda do defendido pela CNPD[32], que só deverá ser permitido e utilizado um único dado biométrico do trabalhador, não nos parecendo admissível o cruzamento de informação deste tipo de informação com outro tipo de tecnologia como é o caso da utilizada pelos meios de vigilância à distância, *inter alia*, a videovigilância ou a geolocalização, ainda que tenha sido acrescentado, e quanto a nós bem, "devendo assegurar-se que apenas se utilizem representações dos dados biométricos e que o respetivo processo de recolha não permita a reversibilidade dos referidos dados".

2.4. O empregador terá, ainda, de respeitar sempre o princípio da proporcionalidade, previsto no art. 5.º, n.º 1, alínea c) do Regulamento Geral. Este princípio é considerado um princípio

[31] Aliás, pode ver-se o mesmo nos arts. 17.º, n.º 2, e 19.º, n.º 3, do CT, assim como no art. 109.º, n.º 2, da Lei 102/2009, de 10 de setembro.
[32] Parecer n.º 20/2018, de 2 de maio deste ano, pp. 37-38.

fundamental, sendo atualmente entendido como um princípio de controlo e um mecanismo de equilíbrio entre os diferentes direitos em causa, e tende a realizar a procura do equilíbrio entre as obrigações do trabalhador, que emanam do seu contrato de trabalho, e o âmbito de liberdade constitucional da sua privacidade, garantindo que a modulação deste direito fundamental vai ser realizada na medida estritamente imprescindível ao seu correto respeito, isto é, com as restrições na quantidade, na qualidade e no procedimento.

No caso dos meios de vigilância à distância a aplicação destes princípios significa que, por exemplo, o controlo do empregador está limitado a determinados espaços geográficos e, por isso, não se poderão colocar câmaras de filmar em certos locais reservados dos trabalhadores como acontece com os lavabos e os vestiários[33], ou mesmo os refeitórios. Estes locais são, por excelência, sítios onde se desenrola a vida íntima ou coletiva dos trabalhadores, resultando claramente que concorre uma dupla situação: por um lado são locais onde não se executa a prestação de trabalho – não são zonas de trabalho da empresa – e, consequentemente, não estão relacionadas diretamente com o cumprimento do objeto do contrato de trabalho; por outro lado, trata-se de espaços em que há uma clara manifestação da intimidade dos trabalhadores.

Atendendo a este facto assemelha-se-nos que a Lei n.º 58/2019, de 8 de agosto, fez bem ao estabelecer no art. 19.º, n.º 2, alínea d), que "As câmaras, ou outros meios de captação de som e imagem, não podem incidir sobre: o interior de áreas reservadas aos trabalhadores, designadamente zonas de refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetas ao seu descanso".

Considera-se positiva esta inclusão como uma forma de reforçar a ideia do respeito pelo princípio da proporcionalidade ainda que nunca tivesse sido admitida a instalação deste tipo de aparelhos nestes espaços.

Por outro lado, significa também que nos dispositivos móveis inteligentes dos trabalhadores não podem ser instalados estes meios de vigilância à distância como é caso de aparelhos de geolocalização, porque são claramente desproporcionais face à finalidade pretendida. Estes dispositivos móveis inteligentes estão intrinsecamente ligados a uma determinada pessoa. A maioria das pessoas mantém os seus dispositivos móveis junto a si, no bolso, na carteira, na roupa que veste e, à noite, próximo da cama, porque têm consciência da quantidade de informação pessoal que os mesmos contêm. Como aponta o GRUPO DE PROTEÇÃO DE DADOS DO ARTIGO 29.º[34], através destes dispositivos móveis inteligentes os fornecedores de serviços de geolocalização obtêm um panorama íntimo dos hábitos e padrões dos proprietários dos mesmos e podem elaborar extensos perfis. Com base no padrão de inatividade durante a noite pode ser deduzido, por exemplo, o local onde dormiram e com base num padrão regular de deslocações de manhã, pode ser inferido, *inter alia*, o local onde trabalham. Este padrão pode

[33] No mesmo sentido, M.ª DO ROSÁRIO PALMA RAMALHO, "Contrato de Trabalho e Direitos Fundamentais da Pessoa", *in Estudos em Homenagem à Professora Doutora Isabel de Magalhães Collaço*, vol. II, Almedina, Coimbra, 2002, pp. 408-409, defende que o direito à reserva sobre a intimidade da vida privada origina a proibição de certas formas de controlo dos trabalhadores, exemplificando com a instalação de câmaras de filmar em locais de repouso ou nos sanitários.

[34] *Parecer n.º 13/2011 sobre serviços de geolocalização em serviços móveis inteligentes*, de 16 de Maio de 2011, p. 7.

incluir, ainda, dados derivados dos padrões de movimentos de amigos com base no chamado *gráfico social*, relacionado com as redes sociais, assim como um padrão de comportamento que pode incluir igualmente categorias especiais de dados, como são os dados sensíveis, se revelar, *inter alia*, visitas a hospitais e a locais de culto religioso ou a presença em manifestações políticas ou noutros locais específicos relacionados, designadamente, com a vida sexual. Acresce, ainda, que estes perfis podem ser utilizados para a tomada de decisões que afetem o proprietário do dispositivo. Por outro lado, é possível, ainda, a monitorização constante dos dados de localização.

2.5. O empregador terá, por último, previamente à adoção de qualquer medida de controlo, de respeitar o princípio da transparência que consiste no conhecimento da vigilância e do controlo exercido pelo empregador, sendo essencial para o correto tratamento de dados pessoais das pessoas, em geral, e dos trabalhadores, em especial, devendo estes saber o como, quando, onde e de que forma o controlo é feito. Este direito, aliás, está reforçado no Regulamento Geral de Proteção de Dados.

Desta forma, todos os tratamentos de dados devem ser comunicados aos trabalhadores devendo ser aprovadas e publicitadas políticas de qualquer monitorização realizada pelo empregador e apenas desde que respeitem estes princípios, sendo que, sempre que possível, os trabalhadores ou os seus representantes devem ser envolvidos na elaboração das mesmas.
E atendendo a este princípio da transparência, no caso da utilização de meios de vigilância à distância, não nos parece que o que consta do art. 20.º, n.º 3 do CT seja suficiente. Na verdade, a informação deve ser mais completa indicando a existência do sistema, a identidade do responsável pelo tratamento que é o empregador, o direito de exercer todos os direitos enquanto titulares de dados pessoais previstos nos arts. 15.º a 22.º do RGPD, desde que adequados à situação concreta.

Tendo em atenção a obrigatoriedade do princípio da transparência e da informação quer aos trabalhadores, quer aos seus representantes, depreende-se não ser admissível o controlo oculto ou secreto sobre os trabalhadores através destes meios por violar o princípio da boa-fé empresarial que tem consagração expressa no CT nos arts. 102.º e 126.º.

2.6. Torna-se ainda importante atender a outro aspeto no tratamento de dados pessoais e, sobretudo, no caso do tratamento através de meios de vigilância à distância na medida em que o art. 28.º, n.º 4 e 5 da Lei n.º 58/2019, de 8 de agosto, estabelece que "As imagens gravadas e outros dados pessoais registados através da utilização de sistemas de vídeo ou outros meios tecnológicos de vigilância à distância, nos termos previstos no artigo 20.º do Código do Trabalho, só podem ser utilizadas no âmbito do processo penal." E n.º 5 "Nos casos previstos no número anterior, as imagens gravadas e outros dados pessoais podem também ser utilizados para efeitos de apuramento de responsabilidade disciplinar, na medida em que o sejam no âmbito do processo penal". Mas só se forem verdadeiros ilícitos penais.

Considera-se positiva esta inclusão pois ao longo do tempo surgiram algumas dúvidas em relação à possível utilização, no exercício do poder disciplinar do empregador, dos dados relativos a incumprimentos contratuais conhecidos de forma acidental, através do controlo destinado a satisfazer as necessidades previstas no art. 20.º, n.º 2, do CT.

Sempre defendemos que, em princípio, a aceitação deste tipo de dados, ainda que captados ocasionalmente para finalidades diferentes das que justificaram a medida inicial, violavam o princípio da finalidade, sendo que a lei não se refere à intencionalidade do sujeito e, por isso, é independente do resultado o facto de ter existido intenção ou não de descontextualizar a informação.

Não parece que possamos retirar do CT a existência de uma exceção ao princípio da finalidade em relação às informações obtidas ocasionalmente que revelem incumprimentos contratuais ou ilícitos sancionados laboralmente. Acresce, ainda, que nos parece que atribuir relevância disciplinar a comportamentos irregulares conhecidos de forma acidental, quando a finalidade da vigilância é outra, equivaleria a assumir também entre os fins da adoção, o controlo do comportamento do trabalhador, o que é claramente interdito pelo art. 20.º, n.º 1, do CT.

Defende-se, assim, por regra, que o princípio da compatibilidade gera a impossibilidade de aplicar aos trabalhadores sanções disciplinares com base em incumprimentos contratuais ocasionalmente captados mediante sistemas de meios de vigilância à distância instalados para cumprir alguma das finalidades previstas no art. 20.º, n.º 2, do CT. Porém, é nosso entendimento que, em determinadas circunstâncias, pode ser lícita a utilização de dados com fins disciplinares quando o que se descobre acidentalmente são factos particularmente gravosos, e que podem constituir ilícitos penais como seria o caso, *inter alia*, de assédio moral, sexual, agressões e furtos.

Contudo, tendo em atenção que este processamento de dados com fins disciplinares constitui uma quebra do princípio da finalidade só pode ocorrer em situações excecionais[35], sendo que esta é a regulamentação que está estabelecida nos n.ºs 4 e 5 da Lei, ainda que se considere que a redação não foi a melhor podendo chegar a originar alguma confusão na mesma.

Conclusões

As TIC e as enormes possibilidades que elas trazem para uma nova sociedade, uma nova economia, e um novo Direito do trabalho, não podem originar que os direitos fundamentais dos trabalhadores, sobretudo o direito à proteção de dados pessoais, volte a ficar *às portas da fábrica*, agora da fábrica *digital*, retrocedendo décadas na interpretação do mesmo.

Parece ser essencial, e mesmo imperioso, refletir sobre a sociedade que queremos construir e onde desejamos viver, sabendo que todas as opções que realizarmos irão influenciar, positiva ou negativamente, as nossas famílias e os nossos descendentes.

O que nos parece essencial nesta matéria é que tenhamos sempre em atenção de que nem tudo o que é tecnicamente possível é juridicamente admissível e que há que respeitar os princípios fundamentais de tratamento de dados pessoais que funcionam como limites ao poder de controlo eletrónico do empregador, quer na fase prévia, quer na fase posterior à

[35] Para maiores desenvolvimentos TERESA COELHO MOREIRA, *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo electrónico do empregador*, Almedina, Coimbra, 2010.

instalação destes dispositivos. Estes princípios mantêm-se, tendo sido até clarificados e aumentados no Regulamento Geral de Proteção de Dados.

Vídeo da apresentação

https://justicatv.com/flv/7npGvYj5SxUUjhDjqYuE5fmT7.mp4

3. A proteção de dados pessoais no contexto das relações laborais

Ana Fernanda Neves

CENTRO
DE ESTUDOS
JUDICIÁRIOS

3. A PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DAS RELAÇÕES LABORAIS*

Ana Fernanda Neves**

1. Introdução

"Os trabalhadores têm o direito de ver os seus dados pessoais protegidos no contexto do emprego"[1], como em outras dimensões da sua vida. As relações laborais são um domínio que envolve um amplo acesso e processamento de dados pessoais, importando para os empregadores a qualidade de responsáveis pelo seu tratamento[2]. No recrutamento, os candidatos a um emprego são chamados a prestar informação sobre as suas qualificações académicas e profissionais e podem, em certos casos, ser sujeito a exames psicotécnicos. Na vigência da relação jurídica, o exercício de direitos pelo trabalhador (por exemplo, do direito de greve e dos direitos de parentalidade) e o cumprimento de deveres pelo empregador em matéria de organização do tempo de trabalho e em matéria de segurança e saúde do trabalho implicam o tratamento de plúrimos dados pessoais. De igual modo, informação pessoal do trabalhador releva na cessação da relação laboral, tenha esta carácter disciplinar ou não (como acontece, por exemplo, quando a idade do trabalhador seja determinante da respetiva

* Apresentação decorrente da ação de formação contínua do CEJ "Proteção de Dados Pessoais", realizada a 19 de junho de 2019.

** Professora da Faculdade de Direito da Universidade de Lisboa.

[1] Princípio 10 ("ambiente de trabalho saudável, seguro e bem-adaptado e proteção de dados"), n.º 3, do Pilar Europeu dos Direitos Sociais. Disponível na internet: <URL: https://ec.europa.eu/commission/publications/european-pillar-social-rights-booklet_en.

[2] É responsável pelo tratamento de dados "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais" (artigo 4.º, 7), do 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 – RGPDP).

reforma ou aposentação) e tal cessação redefine os termos da disponibilidade pelo empregador dos dados pessoais do trabalhador.

A maior relevância hoje do tratamento de dados pessoais nas relações laborais decorre, por um lado, da "crescente digitalização do trabalho" e do facto de a aplicação da tecnologia na organização e realização do trabalho permitirem mais fácil e rápida disponibilidade de dados[3]. Por outro lado, resulta da atualização do regime europeu de proteção de dados pelo Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016[4] (RGPDP), antecedido de jurisprudência significativa do TJUE de aplicação da Diretiva 95/46/CE (que revogou)[5] à luz do artigo 8.º da Carta dos Direitos Fundamentais da União Europeia[6]. Decorre, bem assim, do desenvolvimento jurisprudencial do direito à proteção de dados pelo Tribunal Europeu dos Direitos do Homem (TEDH[7]) no âmbito do artigo 8.º da CEDH, sobre o direito à reserva da vida privada, e da atenção que a matéria tem merecido ao Conselho da Europa, de que é expressiva a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (modernizada pelo Protocolo que a altera em 2018)[8] e a Recomendação CM/Rec(2015)5 sobre o tratamento de dados pessoais no contexto do emprego[9].

Este contexto normativo é determinante para a aplicação das normas nacionais que dispõem sobre a matéria, as quais constituem apenas uma pequena parcela do quadro normativo aplicável às relações laborais (no sector público e privado[10]). Nas normas nacionais, releva o

[3] *V.g.*, Frank Hendrickx, "Article 8 – Protection of Personal Data", *The Charter of Fundamental Rights of the European Union and the Employment Relation*, edited by Filip Dorssemont, Klaus Lörcher, Stefan Clauwaert e Mélanie Schmitt, Hart Publishing, 2019, p. 250 (pp. 249-271); e ponto C.v) da *La Declaración del Centenario de la OIT para el Futuro del Trabajo*, 2019. [Consul. 4 abr. 2020]. Disponível na internet: <URL: https://www.ilo.org/ilc/ILCSessions/108/media-centre/news/WCMS_711408/lang--es/index.htm;
Patricia Vendramin e Gérard Valenduc. *Le travail virtuel. Nouvelles formes d'emploi et de travail dans l'économie digitale,* Étude réalisée pour la Confédération des Syndicats Chrétiens par la *Fondation Travail-Université,* 2016, pp. 8, 10, 11 e 18. [Consul. 4 de abr. 2020]. Disponível na internet: <URL: http://hdl.handle.net/2078.1/174224.

[4] E pelas Orientações emitidas ou renovadas (já depois do RGPDP) do Grupo do Artigo 29.º. Ver artigo 29.º ("Grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais") da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. No âmbito do Regulamento (EU) 2016/679, que revogou aquela Diretiva, cabe ao Comité Europeu para a Proteção de Dados (artigo 68.º) assegurar, para além de outras, as funções cometidas àquele grupo. Entre tais orientações, destaca-se o Parecer n.º 2/2017 sobre o tratamento de dados no local de trabalho, adotado em 8 de junho de 2017, 17/PT, GT 249 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169).

[5] Orla Lynskey, "Delivering Data Protection: The Next Chapter", *German Law Journal*, 2020, Volume 21, Special Issue 1 (20 Challenges in the EU in 2020), pp. 80-84. [Consult. 28 mar. 2020]. Disponível na internet: <URL: https://www.cambridge.org/core/journals/german-law-journal/article/delivering-data-protection-the-next-chapter/2307986C8317AE10B0F98DAACA8BD0ED. Doi:10.1017/glj.2019.100.

[6] Jornal Oficial da União Europeia, 2016/C 202/02.

[7] A Resolução do Conselho de Ministros n.º 21/2019 (Diário da República n.º 20/2019, Série I de 2019-01-29, pp. 586 – 586) determinou, em substituição de direitos do homem, "a adoção da expressão universalista «Direitos Humanos» por parte do Governo e de todos os serviços, organismos e entidades sujeitos aos seus poderes de direção, superintendência ou tutela", aplicando-se apenas a estes.

[8] Texto consolidado disponível na internet: <URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

[9] A qual revê a Recomendação Rec(89)2 sobre a proteção dos dados pessoais utilizados para efeitos de emprego - https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a.

[10] Independentemente da remissão geral do artigo 4.º, n.º 1, da Lei Geral do Trabalho em Funções Públicas (LTFP), anexa à Lei n.º 35/2014, de 20.06 (considerada na versão atualizada), que dispõe ser "aplicável ao vínculo de emprego público, sem prejuízo do [nela] disposto … e com as necessárias adaptações, o disposto no Código do Trabalho e respetiva legislação complementar com as exceções legalmente previstas…", mas por o regime em causa ser sobretudo europeu, aplicando-se às relações laborais do sector privado e do sector público.

disposto no artigo 28.º (relações laborais) da Lei 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679. O artigo 28.º informa que o tratamento de dados pessoais do trabalhador é possível "para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes sectoriais", sem prejuízo das especificidades que estabelece. Estas respeitam, no essencial, à utilização de dados obtidos por "sistemas de vídeo ou outros meios tecnológicos de vigilância à distância" e "ao tratamento de dados biométricos dos trabalhadores".

No presente texto, são analisados os termos da aplicação do regime de proteção dos dados pessoais às relações laborais (**3.**), em três momentos essenciais: o da formação e constituição da relação jurídica de emprego (3.1.), o da execução da relação jurídica (3.2.) e o da sua cessação (3.3.). Particulariza-se ainda o caso da comunicação a terceiros de dados pessoais do trabalhador (como operação de tratamento de dados) no contexto da relação laboral (4.)

Para esta aplicação, importa ter presente a distinção entre o direito à proteção de dados e outros direitos fundamentais com os quais se cruza, designadamente, no domínio laboral, como é o caso do direito à reserva da vida privada, da liberdade de expressão e informação e do direito à não discriminação (**2.**). A esfera de proteção dos dados pessoais assenta num conjunto de subdireitos dos respetivos titulares relativamente aos sujeitos que os tratam. Nesta medida, como se procurará destacar, o regime jurídico da proteção dos dados pessoais, centrado no RGPDP, tem o efeito de reforçar a posição jurídica dos trabalhadores em face dos empregadores (**5.** e **6.**).

2. Delimitação do direito à proteção de dados

2.1. Caracterização geral

Nadezhda Purtova (2018), debruçando-se sobre o conceito de dados pessoais e o impacto deste na garantia do direito à proteção dos dados pessoais, plasticamente escreve[11]:

> "When the hyperconnected onlife world of data-driven agency arrives, the intensive compliance regime of the General Data Protection Regulation (GDPR) will become 'the law of everything', well-meant but impossible to maintain."

A autora questiona a amplitude do conceito, considerando que a complexificação que introduz na proteção dos dados pessoais acabará por ser para a mesma contraproducente[12]. Sendo problemático equacionar um conceito diferente do estabelecido no RGPDP – que os define como consistindo na "informação relativa a uma pessoa singular identificada ou identificável"[13] –, a questão parece residir na própria compreensão do próprio direito. Como refere Aurelia Tamò-Larrieux a locução "proteção de dados" é enganadora, especificando que

[11] "The law of everything. Broad concept of personal data and future of EU data protection law", *Law, Innovation and Technology*, 2018, Vol. 10, No. 1, p. 40 (pp. 40-81).
[Consult. 18 abril. 2020]. Disponível na internet: <URL, https://doi.org/10.1080/17579961.2018.1452176.
[12] "The law of everything….", cit., p. 40.
[13] Artigo 4.º, 1).

"as normas de proteção de dados não protegem os dados em si, mas antes os indivíduos cujos dados são objeto de tratamento"[14].

A proteção de dados pessoais reside no seu tratamento (*v.g.*, recolha, utilização, comunicação, …) correto – com exatidão, "leal e para fins específicos[15] – e na observância de garantias procedimentais[16] que garantam aos titulares um elevado grau de controlo sobre os seus próprios dados, relativamente a qualquer uma das formas pelas quais podem ser processados. Implica que, na vida social, política e administrativa, as pessoas sejam tratadas de forma justa, ou seja, de acordo com seus próprios fatos e atos, no respeito da respetiva identidade pessoal[17]. O direito à proteção de dados pessoais não é, pois, na sua essência, um direito negativo. Pelo contrário, exige dos responsáveis pelo tratamento dos dados uma transparência e cuidados efetivos, no sentido de se certificarem da existência de um título de legitimidade, de garantirem a proporcionalidade do seu tratamento e a precisão dos dados, de assegurarem a "proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental"[18] e, bem assim, no sentido de garantirem aos respetivos titulares o direito de aceder aos dados coligidos que lhes digam respeito, de obter a respetiva retificação e a descontinuação do tratamento quando injustificado[19].

2.2. O direito à proteção de dados pessoais *versus* o direito à privacidade

O direito à proteção de dados pessoais não é, portanto, um direito à privacidade dos dados ou se dilui no direito à reserva da vida privada e familiar. Os direitos são enunciados autonomamente na Carta de Direitos Fundamentais da União Europeia (artigo 7.º, sobre o respeito pela vida privada e familiar; e artigo 8.º, sobre a proteção de dados pessoais); o primeiro está previsto especificamente em algumas Constituições[20]; e a distinção é nomeada em vários instrumentos jurídicos internacionais, como no preâmbulo da Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal modernizada[21].

[14] *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things*, Springer, Nature Switzerland AG, 2018, p. 76.
[15] Artigo 8.º, n.º 2, da CDF.
[16] Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, "The European Union general data protection regulation: what it is and what it means?", *Information & Communications Technology Law*, Volume 28, issue 1, p. 70 (pp. 65-98). [Consult. 18 abr. 2020]. Disponível na internet: <URL https://doi.org/10.1080/13600834.2019.1573501; DOI: 10.1080/13600834.2019.1573501.
[17] Ver, por exemplo, Norberto Nuno Gomes de Andrade, "The Right to Privacy and the Right to Identity in the Age of Ubiquitous Computing", in *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, editado por Christina Akrivopoulou e Athanasios-Efstratios Psygkas, Information Science Reference, Herskey, New York, 2010, pp. 19-42.
[18] Artigo 5.º do RGPDP.
[19] Artigos 16.º a 19.º do RGPDP.
[20] Artigo 37.º e artigo 26.º da CRP.
[21] § 5: "Reconhecendo que é necessário promover a nível global os valores fundamentais de respeito pela privacidade e pela proteção dos dados pessoais, contribuindo assim para o livre fluxo de informação entre as pessoas" (https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016808ac918). De acordo com a Parte 1, n.º 3, da Recomendação CM/Rec/2015)5, "[o] respeito pela dignidade humana, a privacidade e a proteção dos dados pessoais devem ser salvaguardadas no tratamento dos dados pessoais para fins de emprego, nomeadamente para permitir o livre desenvolvimento da personalidade do trabalhador, bem como as possibilidades de relações individuais e sociais no local de trabalho".

Como assinalam Juliane Kokott e Christoph Sobotta, para além de os dados pessoais incluírem informação que não é relativa à vida privada[22] (ver, por exemplo, o Acórdão do TEDH de 8 de novembro de 2016, Magyar Helsinki Bizottság v. Hungary, queixa n.º 18030/11[23]) – sendo portanto o âmbito de aplicação do direito à proteção de dados pessoais mais amplo – e de o direito à reserva da vida privada ser reconhecido às pessoas coletivas, ao invés do primeiro[24], "os requisitos de acordo com os quais os dados pessoais devem ser processados de forma justa e para uma finalidade específica abrangem muitos casos em que uma interferência com a privacidade teria de ser justificada"[25]. Ou seja, há uma lógica positiva que inere ao primeiro – trata-se de saber se, quando e como podem ser tratados dados pessoais e o que o seu titular pode fazer a cada momento relativamente a este tratamento. No caso do direito à privacidade, trata-se de não interferir nesta ou de assegurar a não interferência na esfera pessoal dos indivíduos.

Os direitos intercetam-se "sempre que tenha havido compilação de dados sobre uma determinada pessoa, tratamento ou utilização de dados pessoais ou publicação da informação correspondente de uma forma ou em grau superior ao que seria normalmente previsível"[26]. A "forma ou maneira" como os dados pessoais são tratados releva no ajuizamento sobre a interferência na reserva da vida privada[27]. O TEDH leva em linha de conta, para verificar da aplicabilidade da "noção de 'vida privada', …se os particulares tinham uma expectativa razoável de que a sua vida privada seria respeitada e protegida" (Antović and Mirković v. Montenegro, de 28.11.2017, processo n.º 70838/13, n.º 43). No conceito de vida privada pode ser de incluir "atividades profissionais ou atividades que decorram num contexto público": no caso Antović and Mirković, citado, o TEDH destacou, relativamente à videovigilância de anfiteatros universitários, que estes "são os locais de trabalho dos professores …onde eles não só ensinam os alunos, mas também interagem com eles, desenvolvendo assim relações mútuas e construindo a sua identidade social"; sem que seja possível "distinguir claramente quais das atividades de um indivíduo fazem parte da sua vida profissional ou empresarial e quais não", existindo, antes, "uma zona de interação de uma pessoa com outras, mesmo num

[22] Independentemente das compreensões constitucionais desta. Para uma síntese destas compreensões, ver Manuel José Cepeda-Espinosa, "Privacy", in *Sources of Law and of Rights: Yale Global Constitutionalism,* e*ditor* Judith Resnik, Yale Law School, 2014, pp. I-6-I-8. [Consul. 28 abr. 2020]. Disponível na internet: <URL: https://law.yale.edu/centers-workshops/gruber-program-global-justice-and-womens-rights/global-constitutionalism-seminar/global-constitutionalism-2014-sources-law-and-rights

[23] O TEDH especifica:

> "Although the information request admittedly concerned personal data, it did not involve *information outside the public domain*. As already mentioned above, it consisted only of information of a statistical nature about the number of times the individuals in question had been appointed to represent defendants in public criminal proceedings within the framework of the publicly funded national legal--aid scheme." (itálico nosso)

[24] A este propósito é de notar a falta de base legal para a supressão das decisões judiciais publicadas online do nome das pessoas coletivas (assim como, em regra, das pessoas singulares).

[25] "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law*, 2013, Vol. 3, No. 4, pp. 222-228. Ver, também, United Nations Resolution 42/15, adopted by the Human Rights Council on 26 September 2019, The right to privacy in the digital age, A/HRC/RES/42/15, n.ºs 1 e 2, p. 4. Disponível na internet: <:URL: https://ap.ohchr.org/documents/alldocs.aspx?doc_id=33260.

[26] Acórdão do TEDH de 27.06.2017, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, queixa n.º 931/13, n.º 133.

[27] Acórdão do TEDH de 27.06.2017, Satakunnan Markkinapörssi Oy, n.º 137.
O que em termos práticos obriga os responsáveis pelo tratamento de dados a serem cuidadosos "mais do que impor a cessação de atividades que envolvam dados pessoais" - Aurelia Tamò-Larrieux, *Designing for Privacy*…, cit., p. 74.

contexto público, que pode enquadrar-se no âmbito da 'vida privada'" (n.º 42). Esta compreensão percebe-se melhor se se tiver presente a ausência, na Convenção, datada de 1950, não só do direito à proteção de dados, como de outros que relevam na esfera da preservação da identidade e da esfera de vida pessoal (como o direito ao conhecimento das origens biológicas[28], o direito a ser informado sobre riscos profissionais[29]e o direito ao livre desenvolvimento da personalidade[30]). Na perspetiva do direito à proteção dos dados pessoais, a abordagem ao caso em referência é diferente: implica, primeiramente, que se pergunte sobre a existência de um título jurídico e de uma específica finalidade para a recolha de dados que a colocação do sistema de videovigilância permite[31].

A violação do direito à proteção dos dados pessoais e a violação do direito à reserva da vida privada podem ocorrer isoladamente, verificando uma sem que a outra se verifica; podem ter lugar simultaneamente ou coexistir. Neste caso, não podem, sob pena de imprecisão conceitual e do discurso jurídicos, deixar de ser analisados cada uma por si.

No Acórdão do TEDH de 17.07.2008, I v. Finland, queixa n.º 20511/03. O TEDH concluiu ter sido violada a obrigação positiva do Estado, ao abrigo do artigo 8.º, n.º 1, da CEDH, de assegurar o respeito pela vida privada da queixosa. Destacou que "a necessidade de garantias suficientes é particularmente importante no tratamento de dados muito íntimos e sensíveis, como no caso, em que… a queixosa trabalhou no mesmo hospital onde foi tratada". Notou que a aplicação da lei teria permitido salvaguardar o acesso a informação médica da mesma e que, portanto, o ónus da prova na ação indemnizatória que intentou não podia desconsiderar "as deficiências reconhecidas na conservação dos registos do hospital no momento em que os factos ocorreram" (n.º 44). A legislação nacional, especificou o TEDH, deve "prever garantias adequadas para evitar qualquer comunicação ou divulgação de dados pessoais de saúde que possa ser incompatível com as garantias previstas no artigo 8.º"[32]. À luz do RGPDP, a situação consubstancia a violação do dever de tratamento dos dados pessoais de "uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado" (artigo 5.º, n.º 1, alínea f))[33]. O tratamento de dados por «motivos de saúde» deve ser acompanhado de "medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional"[34] ou deve ter lugar "por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou

[28] Significativamente, Olga Hałub-Kowalczyk (***Redefining the Right to Privacy in the Age of the COVID-19 Pandemic***, Int'l J. Const. L. Blog, Apr. 2, 2020, at: http://www.iconnectblog.com/2020/04/redefining-the-right-to-privacy-in-the-age-of-the-covid-19-pandemic) escreve:

"…privacy became a balloon into which legislators and courts began pumping more and more air. As a result, it became an ever-larger buffer in the relation between the authorities and the individual".

Ver, também, por exemplo, Chris Jay Hoofnagle et al., "The European Union general data protection regulation…", cit., pp. 69-70.

[29] Acórdão de 24.07.2014, Brincat et al. v. Malta, queixas n.ºs 60908/11, 62110/11, 62129/11, 62312/11, 62338/11, n.ºs 103-117.

[30] Acórdão do TEDH de 09.01.2013, Oleksandr Volkov v. Ukraine, queixa n.º 21722/11, n.º 165: o TEDH "[o]bserva que a vida privada 'abrange o direito de um indivíduo a formar e desenvolver relações com outros seres humanos, incluindo relações de natureza profissional ou empresarial' (…). O artigo 8.º da Convenção 'protege o direito ao desenvolvimento pessoal e o direito de estabelecer e desenvolver relações com outros seres humanos e com o mundo exterior' (…). A noção de 'vida privada' não exclui, em princípio, as atividades de natureza profissional ou empresarial."

[31] Artigos 5.º e 6.º do RGPDP.

[32] Acórdão do TEDH de 25.02.1997, Z. v. Finlândia, queixa n.º 22009/93, n.º 95.

[33] No caso, o acesso subsequente a dados de saúde sem salvaguardas.

[34] Artigo 9.º, n.º 2, alínea i), do RGPD.

dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes"[35].

É no plano do respeito do direito à reserva da vida privada que:

a) Se impõe que os empregadores, em regra, se abstenham "de exigir ou solicitar a um trabalhador ou candidato a emprego o acesso a informações que este partilhe com outros em linha, nomeadamente através das redes sociais" (n.º 5.3. da Recomendação CM/Rec(2020)5)[36] e que, em termos gerais, se abstenham de recolher ou relevar informação pessoal usada na sua esfera pública extraprofissional pelo trabalhador, a não ser que esteja em causa o próprio cumprimento de deveres funcionais[37]. Daí ser importante o alcance destes deveres e, portanto, que "os termos e as condições [de um perfil social público conexo ou que contenda com a imagem da empresa fiquem] defini[dos] claramente no contrato de trabalho"[38];
b) Os trabalhadores têm o direito à desconexão digital para além do tempo de trabalho estabelecido legal ou convencionalmente (o que é também uma garantia do direito ao descanso)[39];
c) No contexto do teletrabalho, tem de ser acautelado não só a desconexão digital, mas igualmente a não adoção de medidas intrusivas na "organização do trabalho e das condições de trabalho"[40].

[35] Artigo 9.º, n.º 2, alínea h), e n.º 3, do RGPDP.
O artigo 29.º da Lei n.º 58/2019 refere-se ao tratamento de dados de saúde e dados genéticos. Na verdade, o que está em causa no artigo 9.º do RGPDP é o tratamento de quaisquer dados sensíveis, reportando-se as alíneas h) e i) a contexto de saúde.
Saliente-se a relevância do artigo 29.º, n.º 6, da Lei n.º 58/2019, que estabelece que "[o] titular dos dados deve ser notificado de qualquer acesso realizado aos seus dados pessoais, cabendo ao responsável pelo tratamento assegurar a disponibilização desse mecanismo de rastreabilidade e notificação".
[36] Susana Rodríguez Escanciano, "Posibilidades y límites en el control de los correos electrónicos de los empleados públicos a la luz de la normativa de protección de datos", *Pertsonak eta Antolakunde Publikoak kudeatzeko Euskal Aldizkaria / Revista Vasca de Gestión de Personas y Organizaciones Públicas*, zk/ Núm. 16, 2019, p. 112 (pp. 110-127). [Consult. 18 abr. 2020]. Disponível na internet: <URL https://www.ivap.euskadi.eus/z16-a3rvop/es/contenidos/informacion/16_revgp/es_def/index.shtml. ISSN: 2173-6405; e-ISSN: 2531-2103.
[37] A questão não será, assim, a de indagar se a informação pessoal foi manifestamente tornada pública como é geralmente argumentado (Filipa Urbana Calvão, "A proteção de dados pessoais no contexto laboral: análise da jurisprudência", *CJA*, n.º 128, março/abril, 2018, p. 9; e Teresa Coelho Moreira, "Até que o Facebook nos separe: análise dos acórdãos do Tribunal da Relação do Porto de 8 de setembro de 2014 e do Tribunal da Relação de Lisboa de 24 de setembro de 2014", in *Direitos Fundamentais e de Personalidade do Trabalhador* [em linha], 3.ª edição, Lisboa: Centro de Estudos Judiciários, 2019, p. 44. [consulta 20 mar. 2020]. Disponível na internet. ISBN: 978-989-8908-68-1). A questão é antes a de saber em que medida informação pessoal extrafuncional pode ser considerada pelo empregador no contexto da relação jurídica laboral. É a velha questão, sob nova roupagem, dos deveres extrafuncionais do trabalhador ou antes de saber que condutas exteriores ao local e tempo de trabalho contendem com o cumprimento de deveres funcionais, isto é, deveres relativos ao exercício adequado das funções.
[38] Claudia Ogriseg, "GDPR and Personal Data Protection in the Employment Context", *Labour & Law Issues*, Vol. 3, no. 2, 2017, p. 15. ISSN:2421-2695.
[39] Em Espanha, o direito está expressamente previsto no artigo 88.º, sob a epígrafe "Derecho a la desconexión digital en el âmbito laboral", da Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantia de los derechos digitales. Trata-se de uma decorrência da separação entre o tempo de trabalho e o tempo de descanso e do direito à reserva da vida privada e familiar. A sua inserção naquela lei compreende-se na medida em que constitui também uma lei sobre os direitos digitais dos trabalhadores. O artigo 14.º, alínea j bis), do Real Decreto Legislativo 5/2015, de 30 de octubre (Ley del Estatuto Básico del Empleado Público), estabelece o direito à desconexão digital nos termos estabelecidos na legislação em matéria de proteção de dados pessoais e a garantia dos direitos digitais.

Importa igualmente ter presente que, de acordo com o TEDH, inscreve-se no domínio das obrigações positivas do artigo 8.º da CEDH, garantir a uma pessoa o acesso a informação pertinente e relevante sobre si. Por exemplo, no Acórdão de 07.12.2017, Yonchev v. Bulgária, queixa n.º 12504/09, o TEDH censurou a Bulgária por não ter assegurado ao queixoso, oficial de polícia, um procedimento eficaz e acessível que lhe permitisse ter acesso a informação sobre a avaliação da sua aptidão psicológica realizada como requisito de candidatura a cargo público (n.º 62)[41]. No caso Brincat et al. v. Malta, queixas n.ºs 60908/11 et al., o TEDH, no Acórdão de 4.07.2014, deduziu do artigo 8.º da CEDH o dever positivo do Estado de fornecer informações aos trabalhadores (na situação concreta, de empresa pública) sobre o risco de contacto com amianto a que estavam sujeitos[42].

2.3. O direito à proteção de dados *versus* direito à não discriminação

O direito à proteção de dados pessoais tem um papel relevante na proteção do trabalhador contra a discriminação e a proibição da discriminação (*v.g.*, artigo 21.º da Carta dos Direitos Fundamentais da União Europeia) projeta-se no regime jurídico de proteção de dados. Aquele previne a discriminação, na medida em que importa o tratamento lícito, leal, transparente, com exatidão, limitado a dadas finalidades e mínimo dos respetivos dados[43]. A não discriminação limita a recolha e o tratamento de dados, impedindo a consideração de dados impertinentes, inidóneos, desnecessários e irrazoáveis do ponto de vista da respetiva finalidade. O recurso a motores de busca, palavras-chave e software de pesquisa que envolve inteligência artificial aplicados à ampla informação disponível num ambiente digital e *online* pode gerar problemas de seleção discriminatória de informação e de definição de perfis com efeito discriminatório[44]. Nos termos do artigo 6.º, n.º 1, alínea b), o tratamento de dados pessoais é lícito se necessário no âmbito de "diligências pré-contratuais a pedido do titular dos dados" e, bem assim, no caso da alínea f), se o "tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento…, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa". Atentos os princípios da licitude, lealdade e transparência, limitação das finalidades e minimização, é de concluir[45] que a verificação por um empregador dos "perfis dos candidatos em várias redes sociais" e a inclusão de "informações provenientes destas redes (e quaisquer outras informações disponíveis na *Internet*) no processo de verificação" só será possível "se for necessário para o emprego em questão a análise das informações sobre um candidato nos meios sociais, por

[40] Council of Europe (2020), *Joint statement on the right to data protection in the context of the COVID-19 pandemic, 30 March 2020* [Consult. 12 abr. 2020]. Disponível na internet: <URL: https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter.

[41] No Acórdão de 19.10.2005, Roche v. Reino Unido, de igual modo, o TEDH considerou que o Estado não cumpriu a obrigação positiva, decorrente do artigo 8.º da CEDH, de prever um procedimento eficaz e acessível que permitisse ao requerente, ter acesso a todas as informações pertinentes e adequadas para avaliar qualquer risco a que tenha estado exposto durante a sua participação em 1963 no âmbito de investigação científica sobre armas químicas (n.º 167).

[42] ***Elena Sychenko,*** "Occupational Health in the Jurisprudence of the European Court of Human Rights: Brincat v. Malta", *Strasbourg Observers*, 08.09.2014. [Consult. 12 abr. 2020]. Disponível na internet: <URL: https://strasbourgobservers.com/2014/09/08/occupational-health-in-the-jurisprudence-of-the-european-court-of-human-rights-brincat-v-malta/#_ftnref1.

[43] Artigo 5.º, n.º 1, alíneas a) a d), do RGPDP.

[44] Frank Hendrickx, "Article 8 – Protection of Personal Data", cit., p. 253.

[45] Como exposto no Parecer n.º 2/2017, sobre o tratamento de dados no local de trabalho, p. 13.

exemplo, a fim de poder avaliar os riscos específicos em relação a candidatos para uma função específica, e [se] os candidatos [forem]… corretamente informados (por exemplo, no texto do anúncio de emprego)"[46].

O empregador, para além de acautelar a precisão da informação utilizada, tem de "proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do [trabalhador]… de forma a prevenir, por exemplo, efeitos discriminatórios…contra [os trabalhadores] em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, [mas igualmente de informação sobre o consumo prévio ou atual de álcool ou drogas[47]] ou a impedir que as medidas [técnicas e organizativas utilizadas nos procedimentos de recrutamento ou outros] venham a ter tais efeitos"[48]. O efeito discriminatório pode ser potenciado pelo "tratamento automatizado de dados pessoais", *maxime* quando importe a categorização dos indivíduos quanto a "certos aspetos pessoais", designadamente na perspetiva da análise ou previsão "aspetos relacionados com o seu desempenho profissional, … fiabilidade, comportamento, localização ou deslocações"[49]. Daí a circunscrição dos casos em que decisões inteiramente automatizadas podem ser tomadas[50] e a exigência concomitante da garantia da possibilidade de o trabalhador ou candidato a emprego obter "uma explicação sobre a decisão tomada na sequência dessa avaliação"[51] e "obter intervenção humana por parte do responsável" pelo tratamento dos seus dados, "manifestar o seu ponto de vista e contestar a decisão"[52]. Acresce referir que o risco da discriminação corre por conta do

[46] P. 13.
[47] International Labour Organization, *Management of alcohol- and drug-related issues in the workplace*, 1996, pp. VII, 6 e 21.
[48] Considerando 71, § 2; e considerandos 75 e 85 e artigo 1.º, n.º 2, do RGPDP. Ver, ainda, por exemplo, *Actes du coloque Multiplication des critères de discrimination: enjeux et perspectives*, Le Défenseur des droits, 2018. [Consultta 18 abr. 2020]. Disponível na internet: <URL https://www.ih2ef.education.fr/fr/ressources-par-theme/gestion-des-ressources-humaines/lutte-contre-les-discriminations-au-travail/etat-des-lieux-des-discriminations-dans-la-fonction-publique/.
[49] Artigo 4.º, n.º 4, do RGPDP.
[50] O titular dos dados tem o direito a não ficar sujeito a uma decisão que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como seja um procedimento de recrutamento eletrónico sem qualquer intervenção humana. No entanto, o RGPDP admite a tomada de decisões automatizadas relativamente aos dados não sensíveis em três casos: se for necessário para a celebração ou execução do contrato; se especificamente for admitido por norma jurídica da EU ou nacional, que igualmente preveja medidas de salvaguarda adequadas e se fundada no consentimento explícito do trabalhador (hipótese esta última dificilmente concretizável, atento o valor relativo do consentimento do trabalhador no contexto) – artigo 22.º do RGPDP.
[51] Considerando 71, § 1, do preâmbulo e artigos 13.º, n.º 2, alínea f), 14.º, n.º 2, alínea f), e 15.º, n.º 1, alínea h), do RGPDP.
Assim, por exemplo, relativamente a concurso de colocação de professores, o Conselho de Estado italiano destacou: "…a 'caracterização multidisciplinar' do algoritmo (uma construção que certamente não exige apenas competências jurídicas, mas também competências técnicas, informáticas, estatísticas, administrativas) não dispensa a necessidade de a 'fórmula técnica', que de facto representa o algoritmo, ser acompanhada de explicações que o traduzam na 'regra jurídica' que lhe está subjacente e o tornem legível e compreensível, tanto para os cidadãos como para o juiz" – Sentença de 8 de abril de 2019,
N. 02270/2019REG.PROV.COLL, N. 04477/2017 REG.RIC, n.º 8.3.
Disponível na internet:
<URLhttps://www.giustizia-amministrativa.it/web/guest/dcsnprr?p_p_id=GaSearch_INSTANCE_2NDgCF3zWBwk&p_p_state=normal&p_p_mode=view&_GaSearch_INSTANCE_2NDgCF3zWBwk_javax.portlet.action=searchProvvedimenti&p_auth=Ee24V1nb&p_p_lifecycle=0.
[52] Artigo 22.º, n.º 3, do RGPSP.

empregador, isto é, é ele que tem de demonstrar que adotou medidas que "neutralizem suficientemente" esse risco[53].

2.4. O direito à proteção de dados *versus* liberdade de expressão e de informação

O direito à proteção de dados interfere com a liberdade de expressão e vice-versa[54]**.** Esta "compreende a liberdade de opinião e a liberdade de receber e de transmitir informações ou ideias, sem que possa haver ingerência de quaisquer poderes públicos e sem consideração de fronteiras" e salvaguarda especificamente a liberdade e o pluralismo dos meios de comunicação social (artigo 11.º da CDF; e artigo 10.º da CEDH). O RGPDP impõe que a lei assegure "isenções ou derrogações" a algumas das suas normas, como as relativas aos direitos do titular dos dados (Capítulo III), ao responsável pelo tratamento e subcontratante, as que "forem necessárias para conciliar o direito à proteção de dados pessoais com a liberdade de expressão e de informação", "para fins jornalísticos ou para fins de expressão académica, artística ou literária" (artigo 85.º, n.º 2, do RGPDP). "[A] fim de ter em conta a importância da liberdade de expressão na sociedade democrática, importa interpretar os conceitos relativos a essa liberdade, como o de jornalismo, de modo amplo" – Acórdão do TJUE de 14 de fevereiro de 2019, Sergejs Buivids, C-345/17, n.º 51.

Neste acórdão, o TJUE esclareceu que "[o] artigo 9.° da Diretiva 95/46 [artigo 85.º [tratamento e liberdade de expressão e de informação**]**, n.º 1, do RPDP] deve ser interpretado no sentido de que circunstâncias de facto como as do litígio no processo principal, a saber, a gravação vídeo de agentes da polícia numa esquadra, aquando de uma prestação de declarações, e a publicação do vídeo assim gravado num sítio Internet de vídeos no qual os utilizadores podem carregar, visualizar e partilhar os mesmos, podem constituir um tratamento de dados pessoais para fins exclusivamente jornalísticos…, desde que resulte do referido vídeo que a referida gravação e a referida publicação têm por única finalidade a divulgação ao público de informações, opiniões ou ideias, o que incumbe ao órgão jurisdicional de reenvio verificar"[55].
Por outro lado, uma utilização indevida dos dados pessoais pelo empregador pode ser causa do cerceamento do exercício de direitos pelo trabalhador, como seja a recolha de dados sobre a participação do trabalhador em manifestação ou a expressão da sua opinião contra as condições de trabalho[56].,

[53] Sentença do Tribunal de Haia de 5 de fevereiro de 2020, C-09-550982-HA ZA 18-388 (English), NJCM cs/ De Staat der Nederlanden (NJCM vs the Netherlands), n.º 6.94. Disponível na internet: <URL: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878.
[54] Como destaca Frank Hendricks, "Article 8…", cit., p. 252.
[55] E o TJUE precisou: "55. (…) a circunstância de S. Buivids não ser um jornalista de profissão não é suscetível de excluir que a gravação de vídeo em causa assim como a sua publicação num sítio Internet de vídeos no qual os utilizadores podem carregar, visualizar e partilhar os mesmos possam estar abrangidas por esta disposição. 56. Em especial, o facto de S. Buivids ter publicado esta gravação num tal sítio Internet, neste caso no sítio www.youtube.com, não pode, por si só, retirar a este tratamento de dados pessoais a qualidade de ter sido efetuado «para fins exclusivamente jornalísticos» (…)".
No caso, a Agência Nacional de Proteção de Dados da Letónia considerou, designadamente, que S. Buivids violou o dever, previsto na legislação interna de proteção de dados, de fornecer "aos agentes da polícia, na sua qualidade de pessoas em causa, as informações [nela previstas] … relativamente à finalidade do tratamento dos dados pessoais que lhes diziam respeito".
[56] Freitas v. The Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing and Others (Antigua and Barbuda) [1998] UKPC 30 (30th June, 1998) – https://www.bailii.org/uk/cases/UKPC/1998/30.html.

No caso *Guja v. Moldova* [GC], no. 14277, Acórdão de 12 de fevereiro de 2008, o TEDH declarou que o despedimento do queixoso, Chefe do Departamento de Imprensa da Procuradoria-Geral da República da Moldávia – motivado pelo facto de ter enviado para um jornal duas cartas reveladoras da pressão exercida sobre o Ministério Público por políticos – tinha violado o seu direito à liberdade de expressão, em particular o seu direito de transmitir informações, garantido pelo artigo 10.º da CEDH pois o interesse público na informação em causa se sobrepunha numa sociedade democrático ao interesse na manutenção da confiança naquele serviço. Nesta linha, a Diretiva (EU) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção dos "denunciantes que, trabalhando no setor público ou privado, tenham obtido informações sobre violações em contexto profissional", do Direito da União Europeia (em diferentes domínios, como o dos interesses financeiros da União, o do mercado interno, da proteção do ambiente, da "proteção da privacidade e dos dados pessoais e segurança da rede e dos sistemas de informação", …)[57], precisa que "[a]s pessoas que comunicam informações sobre ameaças ou situações lesivas do interesse público, obtidas no âmbito das suas atividades profissionais, exercem o seu direito à liberdade de expressão" (considerando 31 do preâmbulo). Por outro lado, estabelece que devem existir "procedimentos de proteção adequados para tratar as denúncias e para proteger os dados pessoais das pessoas nelas referidas"[58]. "Os dados pessoais que manifestamente não forem relevantes para o tratamento de uma denúncia específica não devem ser recolhidos ou, se inadvertidamente tiverem sido recolhidos, devem ser apagados sem demora indevida"[59].

No mesmo sentido, a Recomendação CM/Rec(2014)7 do Comité de Ministros aos Estados-Membros relativa à proteção dos denunciantes[60], acautela a proteção do trabalhador neste contexto. Dispõe, designadamente que: *i)* o empregador não deve poder invocar as obrigações legais ou contratuais para impedir o trabalhador de fazer uma declaração ou divulgação de interesse público ou para a penalizar por o ter feito (IIII.11); *ii)* "Os denunciantes devem ser protegidos contra qualquer forma de retaliação, direta ou indireta, pelo seu empregador e pelas pessoas que trabalham para o empregador ou agem em seu nome"[61] (VII.21). O Parecer 2/2017, do Grupo do Artigo 29.º, alerta para a necessidade de acautelar que a monitorização no local de trabalho não dissuade o trabalhador de denunciar práticas ilícitas ou irregularidades[62]. No caso dos empregadores públicos, atentas as obrigações europeias e

[57] Artigos 4.º e 2.º.
[58] Nos termos do RGPDP e da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho (de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes) – n.º 76.
[59] Artigo 17.º, § 2.
[60] Https://cedem.org.ua/en/library/recommendation-cm-rec-2014-7-of-the-committee-of-ministers-to-member-states-on-the-protection-of-whistleblowers/.
[61] "As formas dessa retaliação podem incluir despedimento, suspensão, despromoção, perda de oportunidades de promoção, transferências punitivas e reduções ou deduções de salário, assédio ou outro tratamento punitivo ou discriminatório."
[62] No § último do n.º 4, p. 12 precisa-se:
> "A utilização extensiva das tecnologias de monitorização pode também limitar a disponibilidade dos empregados para (e os canais através dos quais poderiam) informar os empregadores sobre irregularidades ou medidas ilícitas dos superiores e/ou outras ameaças aos empregados para prejudicar a empresa (em especial, os dados do cliente) ou o local de trabalho. O anonimato é muitas vezes necessário para um empregado em causa tomar medidas e comunicar tais situações. A monitorização que atente contra o direito de privacidade dos empregados pode impedir as comunicações necessárias aos responsáveis adequados. Em tal caso, os meios estabelecidos para os autores de denúncia internos podem tornar-se ineficazes."

A proteção é do denunciante, mas igualmente do denunciado, designadamente quanto aos direitos deste à informação, ao acesso, retificação e apagamento dos dados, sem prejuízo de puderem "direitos pode ser objeto de

constitucionais de prestação de informação administrativa ou constante dos arquivos e registos administrativos, a correta aplicação do princípio da minimização conciliado com o princípio da integridade implica que tenham de ser salvaguardados os dados pessoais adequados e necessários, na estrita medida, ao cumprimento de tais deveres e, portanto, veda a anonimização, a destruição e a recusa injustificadas, lesivas do direito à informação.

Vista a distinção e interseções entre o direito à proteção de dados pessoais e os outros direitos fundamentais com os quais se cruza, importa agora precisar a medida da proteção dos dados pessoais nos três momentos estruturais das relações laborais, o da sua formação e constituição (3.2.), o da sua vigência (3.3.) e a da sua extinção (3.4.). Antes, porém, atento o carácter transversal e decisivo para a compreensão e aplicação do RGPDP dos princípios deste[63], há que primeiramente os considerar (3.1.).

3. A proteção de danos pessoais e a «vida» da relação laboral

3.1. Princípios gerais

Os princípios estabelecidos no artigo 5.º do Regulamento (EU) 2016/679 são determinantes para a possibilidade e para a medida do tratamento de dados pessoais (também) no contexto do emprego.

Os dados pessoais só podem ser "recolhidos para finalidades determinadas, explícitas e legítimas", sem que possam ser "tratados posteriormente de uma forma incompatível com essas finalidades" (artigo 5.º, 1), alínea b), do RGPDP)[64]. A licitude da recolha e tratamento para fins de emprego depende da verificação de uma das situações previstas nos artigos 6.º e 9.º da RGPD, sem prejuízo de outras previstas na lei[65]. Em relação aos dados pessoais em geral do trabalhador, decorre do artigo 6.º, n.º 1, alínea a), que é lícito o respetivo tratamento se "for necessário para a execução" do contrato ou relação de trabalho ou no quadro do procedimento de recrutamento e formativo desta, por implicarem "diligências pré-contratuais" que têm lugar na sequência da manifestação de vontade em participar no mesmo ("a pedido do titular dos dados"). O tratamento é lícito também se "for necessário para o

restrição em casos muito específicos, para que se alcance um equilíbrio entre o direito à privacidade e os interesses perseguidos pelo sistema" (GT 29, *Parecer 1/2006 sobre a aplicação das regras europeias em matéria de proteção de dados aos sistemas internos de denúncia de infrações nos domínios da contabilidade, dos controlos contabilísticos internos, da auditoria, da luta contra a corrupção e do crime bancário e financeiro*, GT 117, 1 de fevereiro de 2006) – https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm.

[63] "[O]s princípios fundamentais da legislação em matéria de proteção de dados estabelecidos no artigo 5.º GDPR oferecem uma oportunidade para moldar o ambiente de processamento de dados" (Orla Lynskey, "Delivering Data Protection: The Next Chapter", *German Law Journal*, 2020, Volume 21, Issue 1, p. 83 (pp. 80–84). [Consult. 18 mar. 2020]. Disponível na internet: doi:10.1017/glj.2019.100). São um "um conjunto apelativo de proteções materiais e processuais contra o poder das empresas com utilização intensiva de dados" (
Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, "The European Union general data protection regulation: what it is and what it means", *Information & Communications Technology Law*, 2019, Volume 28, Issue 1, p. 77 (pp. 65-98. [Consult. 18 mar. 2020]. Disponível na internet: DOI: 10.1080/13600834.2019.1573501.

[64] "Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. (…)".

[65] Os dados pessoais devem ser "objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei" (artigo 8.º, n.º 2, da CDFUE). Ver também artigo 35.º, n.ºs 2 e 4, da CRP.

cumprimento de uma obrigação jurídica a que o [empregador]… esteja sujeito" (n.º 1, alínea c)); para o prosseguimento de "interesses legítimos" do empregador ou a cargo de terceiros, "exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do [trabalhador]… que exijam a proteção dos dados pessoais" (n.º 1, alínea f)). No que se refere ao tratamento de dados sensíveis[66], a premissa legal é a de requerem uma proteção mais rigorosa, por o seu tratamento comportar riscos em termos de privacidade e segurança dos indivíduos[67]. Assim, o mesmo só é lícito se "for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do [empregador]… ou do [trabalhador]… em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do [trabalhador, no caso]…" e se "o tratamento for necessário para efeitos de medicina preventiva ou do trabalho [e] para a avaliação da capacidade de trabalho do empregado... com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde"[68]. Em sentido próximo dispõe a Recomendação CM/Rec(2015)5, citada, sobre o tratamento de dados pessoas no contexto do emprego (9.1.), especificando que, "[e]m conformidade com o direito interno, a um trabalhador ou candidato a emprego só podem ser colocadas questões relativas ao seu estado de saúde e/ou ser objeto de um exame médico quando esteja em causa "a sua aptidão para um emprego atual ou futuro"[69]; exigências de medicina preventiva; "garantir uma reabilitação adequada ou cumprir quaisquer outros requisitos em matéria de ambiente de trabalho"; salvaguardar "interesses vitais da pessoa em causa ou de outros trabalhadores e indivíduos"; decidir sobre a atribuição de "benefícios sociais"; "responder a procedimentos judiciais" (9.2.). Em relação aos dados genéticos, precisa que, em regra, os mesmos "não podem ser tratados, por exemplo, para determinar a aptidão profissional de um empregado ou de um candidato a emprego, mesmo com o consentimento da pessoa em causa"; salvo "em circunstâncias excecionais, por exemplo para evitar qualquer prejuízo grave para a saúde da pessoa em causa ou de terceiros, e apenas se estiver previsto na legislação nacional e sujeito a salvaguardas adequadas" (9.3).

Outro princípio fundamental do RGPDP é o princípio da "minimização dos dados", de acordo com o qual só podem ser tratados os dados "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades" que justificam o seu tratamento (artigo 5.º, n.º 1, alínea c), do RGPDP). Como concretiza a Recomendação RM/rec(2015)5[70], os "dados pessoais recolhidos pelos empregadores para efeitos de emprego devem ser relevantes e não excessivos, tendo em conta o tipo de emprego, bem como a evolução das necessidades de informação do empregador" (5.2). A conservação dos dados está limitada pelo princípio da

[66] São os dados "que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical", os dados genéticos, os dados biométricos e os dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa – artigo 9.º, n.º 1, do RGPDP.

[67] Elif Mendos Kuskonmaz e Elspeth Guild, "Covid-19: A New Struggle over Privacy, Data Protection and Human Rights?", 4 may 2020, *European Law Blog, News and Comments on EU Law*. [Consul. 5 mai. 2020]. Disponível in https://europeanlawblog.eu/2020/05/04/covid-19-a-new-struggle-over-privacy-data-protection-and-human-rights/#more-6249.

[68] Artigo 9.º, n.º 2, alíneas b) e h), do RGPD.

[69] Artigo 6.º, n.º 1, alínea d) (exame médico), da Portaria n.º 125-A/2019, de 30.04: "avaliar as condições de saúde física e psíquica dos candidatos exigidas para o exercício da função".

[70] Em termos gerais, estabelece: "[o]s empregadores devem reduzir ao mínimo o tratamento de dados pessoais apenas aos dados necessários para o objetivo prosseguido nos casos individuais em questão" (4.1.).

finalidade e da proporcionalidade (5.3, 1.ª parte). Quando estejam em causa "dados de avaliação relativos ao desempenho ou ao potencial de um trabalhador, esses dados só devem ser utilizados para efeitos de avaliação das competências profissionais" (5.5).

Do ponto de vista dos títulos jurídicos para o tratamento de dados pessoais no emprego, é de salientar que o consentimento é, em regra, um título jurídico não idóneo para o justificar. Como esclarece o Grupo de Trabalho do Artigo 29.º, nas Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, de 2017, atualizadas em 2018, "[a]tendendo à dependência que resulta da relação empregador/trabalhador, é improvável que o titular dos dados possa recusar ao seu empregador o consentimento para o tratamento dos dados sem que haja medo ou risco real de consequências negativas decorrentes da recusa"[71]. Considera, assim, "problemática a questão de os empregadores procederem ao tratamento de dados pessoais dos seus trabalhadores atuais ou futuros com base no consentimento, uma vez que é improvável que esse consentimento seja dado de livre vontade". E precisa ainda que, dado o "desequilíbrio de poder entre empregadores e empregados, estes só podem dar o seu consentimento livremente em circunstâncias excecionais, quando o ato de dar ou recusar o consentimento não produza quaisquer consequências negativas" [72]. É, por exemplo, o caso do consentimento do trabalhador para a colocação de fotografias no diretório da empresa[73]. É a esta luz que tem de ser interpretado e aplicado o disposto no artigo 28.º, n.º 3, da Lei n.º 58/2019, de 8 de agosto[74], que parece circunscrever as situações em que o consentimento não pode ser utilizado, ao limitar as mesmas àquelas em que do tratamento dos dados "resultar uma vantagem jurídica ou económica para o trabalhador", àquelas em que o mesmo influencia o recrutamento e a constituição de relação jurídica de emprego e, bem assim, em que uma "norma legal em contrário" o preveja.

O RGPDP dedica o artigo 88.º, n.º 1, ao tratamento de dados pessoais no contexto laboral[75]. Nos termos deste, os ordenamentos jurídicos nacionais ou através de convenção coletiva podem prever "normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral", designadamente, para efeitos de:

i) Recrutamento;

[71] E concretiza: "É improvável que um trabalhador responda livremente ao pedido de consentimento do empregador para, por exemplo, ativar sistemas de controlo como a observação do local de trabalho através de câmaras ou preencher formulários de avaliação, sem sentir qualquer tipo de pressão para dar esse consentimento".
[72] No caso das relações jurídicas de emprego público, ao desequilibro assinalado ajusta-se o de uma relação com uma entidade pública, como assinala o considerando 43 do preâmbulo do RGPDP, que assinala: "A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. (…)".
[73] Agência dos Direitos Fundamentais da União Europeia, *Handbook on European data protection law, 2018*, edition, p. 145; ver, ainda, pp. 143-144 e p. 330.
[74] Margot E. Kaminski, "The Right to Explanation, Explained", *Berkeley Technology Law Journal*, Volume 34, 2019, p. 195 ("…both Recitals and Working Party/Data Protection Board guidelines play a significant role, in practice, in guiding how companies will behave"). [Consult. 18 abr. 2020]. Disponível na internet: <URL https://scholar.law.colorado.edu/articles/1227.
[75] Ver, também, considerando 155 do RGPDP.

ii) "Execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas";
iii) "Gestão, planeamento e organização do trabalho";
iv) "Igualdade e diversidade no local de trabalho";
v) "Saúde e segurança no trabalho";
vi) De proteção dos bens do empregador ou do cliente;
vii) "Para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego";
viii) E "para efeitos de cessação da relação de trabalho". As normas respeitam à adoção de "medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados", com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho" (n.º 2).

Independentemente da adoção de normas jurídicas neste contexto pelos Estados, o alcance da aplicação do RGPDP no domínio do emprego é-nos dados, em grande medida, pela Recomendação Rec(2015)5, como destacado.

A transparência é outro dos princípios básicos do RGPDP[76]. Margot E. Kaminski refere que "pode ser surpreendente para uma audiência americana quanto dos direitos da RGPDP parecem leis do governo aberto, mais do que motivos para as tradicionais ações sobre privacidade"[77]. Nota que o regime de proteção de dado assenta na ideia de um tratamento leal e justo[78], que "a transparência e a equidade são ideais ligados"; e que, "muitas vezes a transparência é um elemento de responsabilização", determinante para que os sistemas sejam justos[79].

Entre o mais, destaca-se:

i) O tratamento de dados tem de ser, não só lícito, como claro e preciso[80];
ii) Os titulares de dados veem reforçados os seus direitos relativamente aos seus próprios dados, como o direito de ser informados sobre o respetivo tratamento[81] - incluindo sobre os "riscos, regras, garantias e direitos relacionados com o tratamento de dados pessoais, bem como da forma como podem exercer os seus direitos em relação ao tratamento dos dados"[82] -, o direito de acesso aos mesmos, o direito à respetiva portabilidade e o direito a que sejam retificados e, portanto, sejam considerados com exatidão[83];

[76] Margot E. Kaminski, "The Right to Explanation…", cit., p. 209. A Sentença do Tribunal de Haia de 5 de fevereiro de 2020, C-09-550982-HA ZA 18-388, refere que "[o] princípio da transparência é o principal princípio de proteção de dados que está subjacente e estabelecido na Carta e no RGPDP" (n.º 6.86).
[77] *The Right to Explanation…*, cit., p. 209.
[78] Artigo 5.º, n.º 1, alínea a), do RGPDP.
[79] *The Right to Explanation…*, cit., p. 209.
[80] Artigo 5.º, n.º 1, alíneas a) e d), do RGPDP.
[81] Artigos 12.º a 14.º do RGPDP.
[82] Sentença do Tribunal de Haia de 5 de fevereiro de 2020, C-09-550982-HA ZA 18-388, n.º 6.31.
[83] Artigos 5.º, n.º 1, alínea d), e 15.º a 20.º do RGPDP.

iii) O dever de registo das atividades de tratamento[84];
iv) O contrapeso à intervenção (insuficiente ou excessiva) das autoridades nacionais de controlo da aplicação do RGPDP por parte do Comité Europeu para a proteção de dados[85].

Neste contexto, relativamente ao uso de dispositivos de controlo tecnológico de propriedade do empregador, *Cristóbal Molina Navarrete* destaca que "a garantia mais elementar da legitimidade de [tal] uso…é a transparência", *maxime* traduzida na prestação de informação útil, prévia e específica sobre os respetivos fim e modo[86]. No Acórdão de 17 de outubro de 2019, López Ribalda et al. v. Espanha, [GC] queixas n.ºs 1874/13 e 8567/13, o TEDH sublinhou precisamente "que a exigência de transparência e o consequente direito à informação são de natureza fundamental, particularmente no contexto das relações de trabalho, em que a entidade patronal tem poderes significativos em relação aos trabalhadores e qualquer abuso desses poderes deve ser evitado" (n.º 131)[87].

Consideremos, agora, a aplicação do RGPDP em cada um dos momentos essenciais de uma relação laboral.

3.2. A formação e a constituição da relação jurídica laboral

O procedimento de recrutamento ou de formação da relação jurídica e a sua constituição implicam a recolha e subsequente tratamento pelo empregador de dados pessoais (respetivamente, por exemplo, de um lado, informação sobre as habilitações académicas e a morada física ou eletrónica, para efeitos de notificação; e, por outro, a indicação do número de contribuinte, necessário para efeitos da retenção na fonte de imposto sobre o rendimento do trabalho; e a indicação do número de identificação bancário, para pagamento da remuneração)[88]. Os dados que o empregador pode obter e tratar são apenas os adequados e necessários para o efeito[89]. Deste modo, não é possível, em sede de recrutamento, solicitar ao candidato informação sobre, por exemplo:

i) O seu número de contribuinte[90];
ii) Em regra, informação sobre a sua idade[91], salvo se, para além de previsão legal, esta for admissível nos termos da Diretiva 2000/78/CE[92];

[84] Artigo 30.º do RGPDP.
[85] *V.g.*, artigo 70.º, n.º 1, alíneas a), k) e t), do RGPDP.
[86] "Control tecnológico del empleador y derecho probatório: efectos de la prueba digital lesiva de derechos fundamentales", *Temas Laborales, Revista Andaluza de Trabajo y Bienestar Social*, 150, 2019, *Monográfico sobre las facultades de control empresarial ante los cambios tecnológicos y organizativos*, p. 332 (pp. 331-354). [Consulta 3 abr. 2020]. Disponível online in https://dialnet.unirioja.es/ejemplar/536375.
[87] N.º 131.
[88] Artigo 6.º, n.º 1, alíneas b), e f), do RGPP.
[89] Artigo 5.º, n.º 1, alínea c), do RGPDP.
[90] Relevante apenas aquando da constituição do vínculo relativamente ao candidato selecionado.
[91] Declarado que seja o preenchimento da idade mínima legalmente exigida.
[92] Uma característica relacionada com idade, na medida em que "constitua um requisito essencial e determinante para o exercício" de uma atividade profissional ou no "contexto da sua execução", pode justificar diferenciação em razão da idade dessa atividade, desde que, para além de ser legítimo o objetivo, o requisito não seja desproporcionado (artigo 4.º, n.º 1). O artigo 6.º, n.º 1, da mesma Diretiva, que prevê a possibilidade de diferença de tratamento baseadas na idade se "forem objetiva e razoavelmente justificadas, no quadro do direito nacional,

iii) Nem informação sobre a nacionalidade, que, em regra, não pode ser exigida aos nacionais dos Estados-Membros da União Europeia[93], nem, senão em casos limitados, à luz do disposto no artigo 15.º, n.º 2, da CRP, aos nacionais de Estados terceiros;
iv) Informação curricular se a seleção compreender apenas prova de conhecimento ou outros métodos para os quais aquela informação seja irrelevante[94];
v) Informação sobre a vida privada ou pessoal do trabalhador salvo se na medida em que seja "estritamente necessária e relevante para avaliar da respetiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a respetiva fundamentação"[95];
vi) Informação sobre a "sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à natureza da atividade profissional o justifiquem e seja fornecida por escrito a respetiva fundamentação"[96];
vii) Bem assim, não podem ser colocadas questões (designadamente, nas entrevistas) sobre assuntos não relevantes para o emprego[97].

Neste quadro, impõe-se igualmente estar atento à idoneidade dos formulários de participação nos procedimentos de recrutamento e salvaguardar a desnecessidade de preenchimento de campos que são irrelevantes do ponto de vista da informação necessária[98]. O mesmo se diga quanto aos documentos com dados pessoais em geral[99]. De igual modo, no que se refere aos "dados relativos à saúde": nos procedimentos cuja seleção compreende um exame médico, por o exercício de atividade exigir certa condição física e psíquica ou importar a avaliação da capacidade do trabalhador[100], tem de ser assegurado que só a informação médica adequada, pertinente e limitada ao necessário é recolhida (artigo 5.º, n.º 1, alínea c), do RGPDP)[101].

A celebração do contrato ou a constituição através de outro título jurídico da relação laboral implica a disponibilização de informação adicional face ao procedimento de recrutamento. É o caso da indicação do número de contribuinte – necessário para a retenção na fonte de imposto sobre o rendimento do trabalho –; do número de identificação bancária – para pagamento da remuneração; do local de residência do trabalhador, por poder relevar para o pagamento de componente da remuneração e considerando a eventualidade de ocorrência de acidente de trabalho.

---

por um objetivo legítimo, incluindo objetivos legítimos de política de emprego, do mercado de trabalho e de formação profissional, e desde que os meios para realizar esse objetivo sejam apropriados e necessários".
[93] *V.g.*, artigo 45.º do TFUE.
[94] Artigos 18.º, 47.º e 266.º da CRP e artigo
[95] Artigo 17.º, n.º 1, alínea a), do Código do Trabalho; artigo 14.º, n.º 1, alínea a), e n.º 2, da Diretiva 2006/54/CE.
[96] Artigo 17.º, n.º 1, alínea b), do Código do Trabalho
[97] *V.g.*, artigo 5.º, n.º 1, alínea b), do RGPDP; e artigo 17.º, n.ºs 1 e 2, do Código do Trabalho.
[98] Cumpre, pois, aplicar com as devidas cautelas e adaptações do artigo 19.º da Portaria n.º 125-A/2019, de 30.04. As exigências do seu preenchimento devem, em qualquer caso, respeitar o princípio da minimização. A correta aplicação deste princípio dispensa anonimizações injustificadas e lesivas do direito à informação.
[99] Ver, por exemplo, artigo 20.º, n.º 8, da Portaria n.º 125-A/2019, de 30.04.
[100] *V.g.*, artigo 9.º, n.º 2, alínea h), e artigo 6.º, n.º 1, alínea d), da Portaria n.º 125-A/2019, de 30.04; artigos 17.º, n.º 1, alínea b), 19.º, n.º 1, e n.º 2, 225.º, n.º 2, do Código do Trabalho.
[101] Acórdão do TEDH de 29.04.2014, L.H. v. Latvia, queixa n.º 52019/07, n.º 58.
Ver, ainda, por exemplo, Raquel Poquet Catalá, "Vigilancia de la salud, poder de dirección empresarial y derecho a la intimidad del trabajador, un triángulo conflictivo", *Lex Social, Revista Juridica de los derechos sociales*, vol. 10, núm. 1 (2020), pp. 401-403 (pp. [Consulta 20 abr. 2020]. Disponível na internet: https://www.upo.es/revistas/index.php/lex_social.

De acordo com o artigo 10.º do RGPD, o "tratamento de dados pessoais relacionados com condenações penais e infrações ou com medidas de segurança conexas com base no artigo 6.º, n.º 1, [designadamente, se o "tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros"] só é efetuado sob o controlo de uma autoridade pública ou se o tratamento for autorizado por disposições do direito da União ou de um Estado-Membro que prevejam garantias adequadas para os direitos e liberdades dos titulares dos dados". Uma das questões que se suscita relativamente ao artigo 10.º do RGPDP é a de saber se entre as infrações referidas na norma se devem incluir as infrações disciplinares. O Tribunal de Primeira Instância de Amesterdão, em decisão de 23 de dezembro de 2019 – Rb. Amsterdam – C/13/663563 / HA RK 19-97 –, no quadro de ação civil intentada por médico dentista contra a Google no sentido da remoção de todos os resultados relacionados com o seu nome e com as medidas disciplinares aplicadas pelo *Regional Health Care Disciplinary Boards in Amsterdam and Zwolle*, precisou que "[n]ão há qualquer indicação no historial jurídico da GDPR de que os dados pessoais disciplinares sejam qualificados como dados pessoais especiais ou criminais na aceção dos artigos 9.º e 10 da GDPR devido à sua natureza", pelo que decidiu não aplicar ao caso "o quadro de avaliação específico que estes artigos implicam"[102]. Acresce referir que, partir da comparação com as diferentes versões linguísticas, apura-se, com relevância, o seguinte: na versão inglesa, a norma refere-se a "criminal convictions and offences or related security measures"; na francesa a "condamnations pénales et aux infractions ou aux mesures de sûreté connexes"; na espanhola, a "condenas e infracciones penales o medidas de seguridade"; e na versão italiana a "condanne penali e ai reati o a connesse misure di sicurezza". Ou seja, na economia da norma, está-se, no domínio da responsabilidade criminal[103]. As condenações disciplinares e a informação relativa à pendência de procedimentos disciplinares não se inscrevem, pois, no âmbito do artigo 10.º do RGPD, mas relevam nos termos gerais do artigo 6.º do RGPDP.

3.3. O tratamento de dados pessoais durante a vigência da relação jurídica laboral

a) Aspetos gerais

A execução do contrato ou relação de trabalho, o cumprimento da legislação laboral pelos empregadores e o controlo deste cumprimento e "interesses legítimos" dos mesmos torna necessário o tratamento de dados pessoais dos trabalhadores[104]. A título de exemplo, estes dados relevam nos seguintes termos:

i) Em sede de cumprimento de deveres dos trabalhadores, por exemplo, dos deveres de assiduidade e pontualidade;
ii) Para garantia do direito ao descanso e de separação entre o tempo de trabalho e o tempo de descanso, o que reclama "um sistema objetivo, fiável e acessível que

[102] Ver ponto 4.8. do caso - https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/663563_/_HA_RK_19-97.
[103] A partir da versão inglesa, Detlev Gabel e Tim Hickman escrevem, relativamente ao artigo 10.º: "[t]he restrictions concerning the processing of personal data relating to criminal offences or convictions, and civil law enforcement matters" – "Chapter 7: Lawful basis for processing – Unlocking the EU General Data Protection Regulation", [Consult. 17 abr. 2020]. Disponível na internet: <URL: https://www.whitecase.com/publications/article/chapter-7-lawful-basis-processing-unlocking-eu-general-data-protection.
[104] Artigo 6.º, alíneas b), c) e f), do RGPD.

permita medir a duração do tempo de trabalho diário prestado"[105]. Por exemplo, "os dados pessoais que constam do registo dos tempos de trabalho são recolhidos para garantir o cumprimento da legislação relativa às condições de trabalho" e a sua colocação "à disposição da autoridade nacional com competência para a fiscalização das condições de trabalho…, a fim de permitir a sua consulta imediata, na medida em que essa obrigação seja necessária para o exercício, por essa autoridade, da sua missão de fiscalização da aplicação da legislação em matéria de condições de trabalho, nomeadamente, no que respeita ao tempo de trabalho" fundam-se no cumprimento de uma obrigação legal à qual o empregador está sujeito e é necessário para a execução de uma missão de interesse público e exercício da autoridade pública por tal autoridade fiscalizadora (Acórdão de 30.05.2013, C-342/12, Worten - Equipamentos para o Lar, SA contra Autoridade para as Condições de Trabalho, n.ºs 34-45).

iii) Para a realização de descontos facultativos, como é o caso de quotização associada a filiação sindical do trabalhador, se essa for a vontade do trabalhador[106];

iv) Para o exercício de certos direitos, por exemplo, no âmbito da tutela da parentalidade[107]; da justificação de ausências relativas ao exercício da atividade sindical, por casamento[108], …;

v) Por o cumprimento de obrigações jurídicas pelo empregador[109], *v.g.*, realização de descontos obrigatórios para a Segurança Social e do imposto sobre o rendimento das pessoas singulares[110];

vi) O tratamento de dados pessoais é necessário no quadro da avaliação de acumulação de funções públicas com atividade privada e da identificação de incompatibilidades ou de situação de concorrência desleal do trabalhador para com o empregador[111];

vii) Para efeitos de avaliação do desempenho, postulando, por exemplo, os princípios do tratamento justo dos dados e da exatidão dos dados" (artigo 5.º, n.º 1, alíneas a) e d), do RGPD), "avaliações justas e honestas" e não ofensivas "na forma como são formulados"[112].

[105] Acórdão de 14.05.2019, Federación de Servicios de Comisiones Obreras (CCOO) contra Deutsche Bank SAE, C-55/18, n.º 65. O TJUE concluiu que "[o]s artigos 3.º, 5.º e 6.º da Diretiva 2003/88/CE do Parlamento Europeu e do Conselho, de 4 de novembro de 2003, relativa a determinados aspetos da organização do tempo de trabalho, lidos à luz do artigo 31.º, n.º 2, da Carta dos Direitos Fundamentais da União Europeia, bem como do artigo 4.º, n.º 1, do artigo 11.º, n.º 3, e do artigo 16.º, n.º 3, da Diretiva 89/391/CEE do Conselho, de 12 de junho de 1989, relativa à aplicação de medidas destinadas a promover a melhoria da segurança e da saúde dos trabalhadores no trabalho, devem ser interpretados no sentido de que se opõem a uma regulamentação de um Estado-Membro que, segundo a interpretação que lhe é dada pela jurisprudência nacional, não impõe às entidades patronais a obrigação de estabelecer um sistema que permita medir a duração do tempo de trabalho diário prestado por cada trabalhador".

[106] *V.g.*, artigos 170.º e 171.º da LTFP; artigo 457.º, n.º 3, artigo 458.º, n.º 8, do Código do Trabalho.

[107] *V.g.*, artigo 35.º do Código do Trabalho e artigo 4.º, n.º 1, alínea e), da LTFP.

[108] *V.g.*, artigo 409.º, artigo 249.º, n.º 2, alínea a), do Código do Trabalho; e artigos 344.º e 345.º e artigo 134.º, n.º 2, alínea a), da LTFP.

[109] *V.g.*, artigo 6.º, n.º 1, alínea c), do RGPD.

[110] *V.g.*, artigo 170.º da LTFP; artigo 276.º do Código do Trabalho.

[111] *V.g.*, artigo 6.º, n.º 1, alíneas b) e) e f), do RGPDP; artigo 128.º, n.º 1, alínea f), do Código do Trabalho; e artigos 19.º a 24.º da LTFP; sem prejuízo da necessária contextualização deste nos parâmetros decorrentes da Diretiva (UE) 2019/1152 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa a condições de trabalho transparentes e previsíveis na União Europeia.

[112] Como precisa o *Handbook on European data protection law,* cit., p. 334.

b) O tratamento de dados pessoais do trabalhador por razões de saúde e segurança no trabalho

No contexto do emprego, o tratamento de dados pessoais é necessário para o cumprimento das obrigações do empregador relativas à saúde e segurança no local de trabalho e pode-o ser por razões de interesse público relativas ao controlo de doenças e outras ameaças para a saúde (artigo 9.º, n.º 2, alíneas b) e i), do RGPDP); se "for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde…" (artigo 9.º, n.º 2, alínea h), do RGPSP); e se o tratamento for "necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular", sem que seja possível obter o consentimento do titular dos dados, por "estar física ou legalmente incapacitado de dar o seu consentimento" (artigo 9.º, nº 2, alínea i), do RGPDP). O considerando 46 do preâmbulo do RGPDP esclarece que "[a]lguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação…".

No contexto da prevenção e combate à epidemia por COVID-19, de acordo com o Comité Europeu para a Proteção de Dados, os empregadores podem obter informações pessoais para "cumprir os seus deveres e organizar o trabalho de acordo com a legislação nacional" (*Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020*[113]). Esta, enquadrada por legislação europeia, impõe que o empregador assegure aos trabalhadores "condições de segurança e saúde em todos os aspetos relacionados com o trabalho, aplicando as medidas necessárias tendo em conta princípios gerais de prevenção" (artigo 281.º, n.º 2, do Código do Trabalho)[114]. O "risco Covid-19…embora seja certamente um risco (biológico) não (direta e estritamente) da empresa (exceto, evidentemente, para as empresas do sector da saúde), mas sim externo/geral, transforma-se num risco (genérico, mas agravado) 'interno' para os trabalhadores que a ele podem estar expostos e, consequentemente, deve ser avaliado pelo empregador como um risco (também) da empresa e, neste sentido, específico"[115]. O empregador tem o dever de "[a]ssegurar, nos locais de trabalho, que as exposições aos agentes [entre outros] … biológicos… não constituem risco para a segurança e saúde do trabalhador" (artigo 15.º, n.º 2,

[113] [Consult. 3 abr. 2010]. Disponível na internet: <URL: Https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

[114] *V.g.*, artigo 5.º e 6.º da Diretiva 89/391/CEE, de 12 de junho de 1989, relativa à aplicação de medidas destinadas a promover a melhoria da segurança e da saúde dos trabalhadores no trabalho.

[115] Gaetano Natullo, "Covid-19 e sicurezza sul lavoro: nuovi rischi, vecchie regole?", *WP C.S.D.L.E. "Massimo D'Antona".*IT – 413/2020, p. 12. Elena Poli, Stefania Mangione e Alberto Piccinini destacam que o "risco da exposição a agentes biológicos", tratado na legislação sobre segurança e saúde no trabalho, "inclui certamente a definição de 'COVID-19'", "Emergenza COVID-19 e obblighi di protezione, controlli e gestione della privacy", *Newsletter Wikilabour.it, Il grande dizionario dei diritti dei lavoratori annotato con la giurisprudenza*. [Consult 20 mar. 2020]. Disponível na internet:
<URL: https://www.wikilabour.it/Segnalazioni-Newsletter.ashx?From=Newsletter.
A empresa, através dos seus trabalhadores, pode igualmente ser vista como «exportadora» de riscos - Paolo Pascucci, "Sistema di prevenzione aziendale, emergenza coronavirus ed effettività", *Emergenza COVID-19 Speciale, Uniti per l'Italia*, Giuffrè Francis Lebreve, S.p., Milano, 2020, p. 78. (Giustiziacivil.com, ISSN 2420-9651).

alínea f), da Lei n.º 102/2009, de 10.09)[116] [117]. O trabalhador deve "cooperar ativamente na empresa, no estabelecimento ou no serviço para a melhoria do sistema de segurança e de saúde no trabalho, tomando conhecimento da informação prestada pelo empregador e comparecendo às consultas e aos exames determinados pelo médico do trabalho" e, "em caso de perigo grave e iminente, adotar as medidas e instruções previamente estabelecidas para tal situação, sem prejuízo do dever de contactar, logo que possível, com o superior hierárquico ou com os trabalhadores que desempenham funções específicas nos domínios da segurança e saúde no local de trabalho" (artigo 17.º, n.º 1, respetivamente, alínea d) e alínea f), da Lei n.º 102/2009)[118].

No quadro das várias disposições que obrigam o empregador e o trabalhador[119], observados que sejam os princípios da proporcionalidade e da minimização dos dados, o empregador pode solicitar informações de saúde aos trabalhadores no contexto da COVID-19; pode efetuar "controlos médicos dos trabalhadores"[120]; e "deve informar os trabalhadores sobre os casos COVID-19 e tomar medidas de proteção, mas não deve comunicar mais informações do que as necessárias. Nos casos em que seja necessário revelar o nome do(s) trabalhador(es) que contraiu o vírus (por exemplo, num contexto preventivo) e a legislação nacional o permita, os trabalhadores em causa devem ser previamente informados e a sua dignidade e integridade devem ser protegidas" [121]. A sua comunicação às autoridades públicas deve ocorrer nos estritos limites da respetiva base legal (por exemplo, no quadro do artigo 7.º da Diretiva

[116] De acordo com a Diretiva 2000/54/CE do Parlamento Europeu e do Conselho, de 18.09.2000, relativa à proteção dos trabalhadores contra riscos ligados à exposição a agentes biológicos durante o trabalho, em função da avaliação dos riscos para a segurança ou saúde dos trabalhadores, o empregador deve evitar a respetiva exposição aos mesmos. Não sendo "tecnicamente praticável, tendo em conta a atividade profissional e a avaliação referida… deve ser reduzido a um nível tão baixo quanto for necessário para proteger de maneira adequada a saúde e a segurança dos trabalhadores em causa, particularmente mediante a aplicação" de medidas como a "limitação ao mínimo do número de trabalhadores expostos ou suscetíveis de o ser"; a "conceção de processos de trabalho e medidas técnicas de controlo, a fim de evitar ou minimizar a disseminação de agentes biológicos no local de trabalho"; e a adoção de "medidas de proteção coletivas e/ou medidas de proteção individual, quando a exposição não possa ser evitada por outros meios" e de "medidas de higiene compatíveis com os objetivos de prevenção ou redução da transferência ou disseminação acidental de um agente biológico para fora do local de trabalho" (artigo 6.º, n.ºs 1 e 2, alíneas a) a d)). Deve ser garantida a "vigilância adequada da saúde dos trabalhadores em relação aos quais …[exista]… um risco para a sua segurança ou saúde" (artigo 8.º, n.º 1).

[117] Este dever do empregador é exponenciado por normas específicas adotadas no combate ao COVID-19. É o caso italiano, com o equacionar inclusive da recusa de prestação do trabalho pelo trabalhador no caso de não estarem asseguradas pelo empregador "medidas para combater e conter a propagação do vírus Covid-19 no local de trabalho" - Antonio Pileggi, "Una riflessione sul diritto del lavoro alla prova dell'emergenza Epidemiológica", in *Il Diritto del Lavoro dell'Emergenza Epidemiologica*, a cura di a cura di Antonio Pileggi, Edizioni LPO – Supplemento al n. 3-4/2020 di Lavoro e Previdenza Oggi, 1ª edizione, maggio2020, p. 11. [Consul. 10 mai 2020]. Disponível na internet: <URL: http://csdle.lex.unict.it/docs/generic/Antonio-Pileggi-Il-Diritto-del-Lavoro-dellemergenza-epidemiologica/5993.aspx.

[118] Ver, também, *v.g.*, artigo 13.º da Diretiva 89/391/CEE.

[119] "O trabalhador, assim como os seus representantes para a segurança e para a saúde na empresa, estabelecimento ou serviço, deve dispor de informação atualizada sobre", designadamente, "os riscos para a segurança e saúde, bem como as medidas de proteção e de prevenção e a forma como se aplicam, quer em relação à atividade desenvolvida quer em relação à empresa, estabelecimento ou serviço" e sobre "medidas e as instruções a adotar em caso de perigo grave e iminente" (artigo 19.º, n.º 1, alíneas a) e b), da Lei n.º 102/2009).

[120] Decreto-Lei n.º 20/2020, de 01.05, que altera as medidas excecionais e temporárias relativas à pandemia da doença COVID-19, prevê, no artigo 13.º-C, o controlo da temperatura corporal para acesso e permanência no local de trabalho.

[121] European Data Protection Board (2020), *Statement on the processing of personal data in the context of the COVID-19 outbreak*, 19 March 2020, citado; e Council of Europe (2020), *Joint statement on the right to data protection in the context of the COVID-19 pandemic*, 30 March 2020 [Consult. 12 abr. 2020]. Disponível na internet: <URL: https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter.

2000/54/CE do Parlamento Europeu e do Conselho, citada) e na "perspetiva da adotação de medidas que permitam a retoma ao 'normal' tratamento de dados…uma vez cessado o estado de emergência"[122].

c) O uso da internet e de comunicações eletrónicas no local de trabalho

A prestação de trabalho muitas vezes realiza-se em ambiente tecnológico ("no próprio meio tecnológico"[123]) ou implica a utilização de "dispositivos técnicos e TIC" do empregador (como o uso da Internet e do correio eletrónico) do empregador pelo trabalhador coloca a questão da monitorização do seu uso e do acesso ao conteúdo. O princípio é o de que "[o]s empregadores devem evitar interferências injustificáveis e irrazoáveis com o direito dos trabalhadores à privacidade" (Recomendação Rec(2015)5, n.º 14.1.). Tal significa que:

a) Deve ser prestada informação clara e atualizada aos trabalhadores sobre o uso da Internet e das comunicações eletrónicas no local de trabalho, assim como sobre os termos de tratamento dos dados correspondentes, designadamente informação sobre "o tipo de comunicações" sobre que incide "monitorização"[124], os períodos de conservação dos dados de tráfego e das comunicações eletrónicas profissionais (14.1.)[125];

b) Devem ser adotadas as formas menos intrusivas de tratamento dos dados. Deste modo, havendo "tratamento de dados pessoais relativos a páginas da Internet ou da Intranet a que o trabalhador tenha acesso, deve ser dada preferência à adoção de medidas preventivas, como a utilização de filtros que impeçam determinadas operações e a graduação de eventuais controlos de dados pessoais, dando preferência a controlos aleatórios não individuais de dados que sejam anónimos ou de alguma forma agregados" (14.2.)[126];

c) O acesso dos empregadores às comunicações eletrónicas profissionais dos seus empregados só pode ter lugar se tiverem "sido previamente informados da existência dessa possibilidade" e se "necessário, por razões de segurança ou outras razões legítimas". Estando o trabalhador ausente, o empregador deve prever "procedimentos adequados" para que o "acesso às comunicações eletrónicas profissionais", no caso de

[122] Council of Europe (2020), *Joint statement*…, citado.
[123] Alicia Villalba Sánchez, "El derecho fundamental a la protección de datos del trabajador de datos del trabajador frente a los riesgos de la contratación estandardizada", *Nueva revista española de derecho del trabajo*, n.º 207, 2018, p. 90 (pp. 875-111).
[124] Parecer n.º 2/2017, do Grupo do Artigo 29, cit., p. 17. Como aí se precisa ainda "[u]ma política relativa aos efeitos de quando e por quem podem ser acedidos dados de entrada suspeitos deve ser desenvolvida e tornada acessível, de forma fácil e permanente a todos os empregados, a fim de os orientar também sobre a utilização aceitável e não aceitável da rede e das instalações. Tal permite aos empregados adaptar o seu comportamento para evitarem ser controlados quando legitimamente utilizem as instalações de trabalho de TI para utilização privada".
[125] No Acórdão de 03.04.2007, Copland v. Reino Unido, queixa n.º 62617/00, o TEDH concluiu que a recolha e o armazenamento de dados relativos à utilização do telefone, correio eletrónico e Internet por uma trabalhadora secretária do dirigente máximo de um estabelecimento de ensino superior sem que a lei fosse "suficientemente clara nos seus termos para dar aos indivíduos uma indicação adequada sobre as circunstâncias e as condições em que as autoridades estavam habilitadas a recorrer a tais medidas" (n.º 46) e sem que existissem "disposições no momento relevante, quer no direito interno geral quer nos instrumentos que regem o Colégio, regulando as circunstâncias em que os empregadores podiam controlar a utilização do telefone, do correio eletrónico e da Internet pelos trabalhadores" (n.º 47) violou o artigo 8.º da CEDH (n.º 48).
[126] No mesmo sentido, Grupo do Artigo 29, Parecer n.º 2/2017, p. 19 (que, designadamente, especifica "Se for possível o bloqueio de sítios *Web*, em vez de a monitorização contínua de todas as comunicações, o bloqueio deve ser escolhido, a fim de cumprir este requisito da subsidiariedade."

"necessidade profissional", seja "efetuado da forma menos intrusiva possível e apenas após ter informado os trabalhadores em causa" (14.3).

d) Excluídas de monitorização estão "[o] conteúdo, o envio e a receção de comunicações eletrónicas privadas no trabalho" (14.4.), por, não se reportando ao trabalho, constituírem uma interferência injustificada na vida pessoal do trabalhador.

Os parâmetros expostos estão bem presentes na jurisprudência do TEDH. Considere-se, a título de exemplo, os seguintes casos:

a) No caso Libert v. France, o TEDH destacou que, se um empregador "não pode, em princípio, abrir ficheiros identificados como 'pessoais' pelo trabalhador", no caso concreto, a carta do utilizador para uso do sistema de informação da *Société nationale des chemins de fer* (SNCF) afirmar especificamente que "os dados privados devem ser claramente identificados como tal (entre outros, a opção 'privada' nos critérios de Outlook) [e que] o mesmo se aplica aos meios de comunicação que recebem essa informação (pasta 'privada')" e, bem assim, que o queixoso utilizou uma parte substancial do espaço de armazenamento no seu computador de trabalho para armazenar os ficheiros em questão (1 562 ficheiros representando um volume de 787 megabytes), o que justificou a necessidade de a SNCF e os tribunais nacionais examinarem minuciosamente o caso. Nestes termos, o TEDH, "observando, além disso, que é obrigado a considerar as decisões contestadas à luz do caso na sua totalidade, considera que as autoridades nacionais não excederam a sua margem de apreciação e que, por conseguinte, não houve violação do artigo 8.º da Convenção"[127].

b) No Acórdão de 05.09.2017, Bărbulescu v. Roménia, (GC), n.º 61496/08, o TEDH censurou o facto de os tribunais nacionais não terem determinado: *i)* as razões específicas que justificaram a introdução das medidas de controlo; *ii)* se o empregador poderia ter utilizado medidas menos intrusivas; *iii)* se o requerente tinha sido previamente informado pelo seu empregador da possibilidade de as suas comunicações no Yahoo Messenger, criado para uso profissional na empresa, poderem ser monitorizadas e, bem assim, sobre a natureza ou a extensão da monitorização[128].

O artigo 22.º, n.º 1, do Código do Trabalho[129] deixa claro que o "trabalhador goza do direito de reserva e confidencialidade relativamente ao conteúdo das mensagens de natureza pessoal e acesso a informação de carácter não profissional que envie, receba ou consulte, nomeadamente através do correio eletrónico". As dificuldades residem no controlo da utilização de "dispositivos técnicos e TIC" do empregador pelo trabalhador que não sejam assinaladas pelo trabalhador como pessoais. O Código do Trabalho estabelece que o empregador tem o poder de "estabelecer regras de utilização dos meios de comunicação na empresa [serviço[130]], nomeadamente do correio eletrónico" (artigo 22.º, n.º 2). Tais regras têm

[127] Acórdão de 22 de fevereiro de 2018, queixa n.º 588/13, n.º 52.
[128] N.º 140.
[129] Aplicável ao trabalho em funções públicas *ex vi* artigo 4.º, n.º 1, al. b), da LTFP.
[130] Recorde-se que o artigo 4º, n.º 4, da LTFP estabelece que, "[p]ara efeitos da aplicação do regime previsto no Código do Trabalho ao vínculo de emprego público, as referências a empregador e empresa ou estabelecimento, consideram-se feitas a empregador público e órgão ou serviço, respetivamente".

de ser integradas pelos parâmetros enunciados do Conselho da Europa, acolhidos na jurisprudência do TEDH na aplicação do artigo 8.º da CEDH. De igual modo, à luz dos princípios da finalidade, da minimização e transparência estabelecidos no RGPD[131], é claro que: *i)* o trabalhador tem de ser informado sobre a existência da monitorização, sobre os seus propósitos, sobre o responsável pelo tratamento da informação e sobre a possível relevância da mesma; e *ii)* os termos da monitorização devem ser o menos intrusivos possível face às finalidades que a justificam.

d) Sistemas de informação e tecnologias para monitorizar os trabalhadores, incluindo videovigilância

A Recomendação Rec(2015)5, em referência, estabelece que a introdução e utilização de "sistemas de informação e tecnologias para monitorizar direta e principalmente a atividade e o comportamento dos trabalhadores não devem ser permitidas", assim como o "uso de vídeo para monitorizar a área pessoal dos trabalhadores" (15.1. e 14.2., 2.ª parte).

No entanto, prevê "a sua introdução e utilização para outros fins legítimos, tais como a proteção da produção, da saúde e da segurança ou para assegurar o funcionamento eficiente de uma organização [que] tenha como consequência indireta a possibilidade de controlar a atividade dos trabalhadores" (15.2.). Neste caso:

i) Os trabalhadores devem ser previamente informados (21.a));
ii) Tais sistemas devem ser "especificamente concebidos e localizados de forma a não violar os seus direitos fundamentais" (15.2.);
iii) Os representantes dos trabalhadores devem ser previamente consultados (21.c));
iv) O arquivo das gravações deve ter um tempo limite (15.3.);
v) No caso de disputa ou de processo judicial, os trabalhadores devem ter acesso a cópia das gravações (15.3.).

O TEDH, no Acórdão de 17 de outubro de 2019, López Ribalda et al. v. Espanha, citado, n.º 116, clarificou que, para "garantir a proporcionalidade das medidas de videovigilância no local de trabalho", os tribunais nacionais devem, na ponderação dos interesses concorrentes, verificar os seguintes aspetos:

i) Se o trabalhador foi notificado clara e previamente sobre a sua adoção e natureza;
ii) A extensão da monitorização pelo empregador e o grau de intrusão na privacidade do trabalhador. Neste contexto, o nível de privacidade na área monitorizada deve ser considerado, juntamente com quaisquer limitações de tempo e espaço e o número de pessoas que têm acesso aos resultados;
iii) Se o empregador forneceu razões legítimas para justificar a monitorização e a extensão da mesma. Quanto mais intrusiva for a monitorização, mais relevante terá de ser a justificação;
iv) Se teria sido possível adotar um sistema de monitorização baseado em métodos e medidas menos intrusivas, isto é, se, atentas as circunstâncias particulares de cada

[131] *V.g.*, artigos 5.º, alíneas a), b) e c), e 12.º do RGPDP.

caso, o objetivo prosseguido pelo empregador poderia ter sido alcançado através de um menor grau de interferência na esfera do trabalhador;
v) As consequências da monitorização para o trabalhador a ela sujeito, verificando da sua coerência com o objetivo que a justificou;
vi) A existência de "garantias adequadas", como "a prestação de informações aos trabalhadores em causa ou aos representantes do pessoal sobre a instalação e a extensão da monitorização", a "comunicação de tal medida a um organismo independente" ou a "possibilidade de apresentar uma queixa".

De acordo com o Código do Trabalho, a utilização de "meios de vigilância a distância no local de trabalho, mediante o emprego de equipamento tecnológico", pode ter lugar para "proteção e segurança de pessoas e bens" e por "particulares exigências inerentes à natureza da atividade"[132], com exclusão do controlo do "desempenho profissional do trabalhador"[133]. Em qualquer dos casos, essa utilização tem de ser "necessária, adequada e proporcional aos objetivos a atingir"[134]. Deve ser prestada informação e feita consulta às estruturas representativas dos trabalhadores[135]. As expressões "natureza da atividade", "particulares exigências" e "desempenho profissional" não são inequívocas no seu alcance. Diferentemente, a título de exemplo, o artigo do Real Decreto Legislativo 2/2015, de 23.10, que aprova o "texto refundido de la Ley del Estatuto de los Trabajadores", estabelece:

> "El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad" (artigo 20.º, n.º 3). O artigo 89.º da Ley Orgánica 3/2018, de 5.12, de Protección de Datos Personales y garantia de los derechos digitales, remete para esta norma. O artigo 14.º, j) bis, do Real Decreto Legislativo 5/2015, de 30.10, que aprova o "texto refundido de la Ley del Estatuto Básico del Empleado Público", remete para aquela Ley Orgánica[136].

O princípio da finalidade, do RGPDP, desempenha um papel essencial. Recorde-se que, de acordo com este, os dados pessoais são "[r]ecolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades" (artigo 5.º, n.º 1, alínea b), RGPDP). Tal significa, por exemplo, que se o sistema de

[132] Artigo 20.º, n.º 2, do Código do Trabalho; e *ex vi* artigo 4.º, n.º 1, alínea b), da LTFP.
No que se refere à "natureza da atividade", estar-se-á perante situações em que o cumprimento do objeto do contrato implica a captação de imagens (as quais, para além da sua proteção autónoma – *v.g.*, artigo 26.º, n.º 1, da CRP -, constituem dados pessoais). Alicia Villalba Sánchez, "El derecho fundamental a la protección de datos del trabajador frente a los riesgos de la contratación estandardizada", *Nueva revista española de derecho del trabajo*, n.º 207, 2018, p. 883 (pp. 875-111).
[133] Artigo 20.º, n.º 1, do Código do Trabalho.
[134] Artigo 21.º do Código do Trabalho.
[135] Artigo 466.º, n.º 1, alínea c), e artigos 423.º, n.º 1, alíneas a) e b), e 426.º, n.ºs 1 e 2, alíneas b) e e), do Código do Trabalho.
[136] Estabelece:
"Los empleados públicos tienen los siguientes derechos de carácter individual en correspondencia con la naturaleza jurídica de su relación de servicio: (…) // j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales."

videovigilância é legitimamente instalado para proteger o património do empregador não pode ser utilizado para "monitorizar a disponibilidade, o desempenho e a simpatia dos empregados para com os clientes"[137], mas apenas condutas que relevam para a proteção daquele.

A Lei n.º 58/2019 prevê a utilização das "imagens gravadas e outros dados pessoais registados através da utilização de sistemas de vídeo ou outros meios tecnológicos de vigilância à distância" "no âmbito do processo penal" e, bem assim, que "as imagens gravadas e outros dados pessoais" obtidos nesses termos podem também ser usadas "para efeitos de apuramento de responsabilidade disciplinar", mas, neste caso, acrescenta, "na medida em que o sejam no âmbito do processo penal"[138], parecendo pressupor a existência de um processo penal no qual relevam. O legislador parece ter ido mais longe do que a própria Comissão Nacional para a Proteção de Dados. De acordo com o entendimento, o seu uso é possível quando esteja em causa conduta suscetível de constituir (indiciariamente) crime e a entidade empregadora tenha feito participação criminal[139]. Foi mais longe do que o próprio TEDH, que, no caso López Ribalda et al. v. Espanha, citado, sancionou a aplicação que os tribunais espanhóis fizeram do respetivo regime legal, acima referido, centrado sobre a "extensão e limites da garantia de transparência como condição para a validade e eficácia das provas tecnológicas em geral e da videovigilância em particular"[140] e não, como o regime português, sobre a circunscrição dos casos em que pode ser utilizado, que, no essencial, se resume às situações com relevância criminal. Diferente é a situação da utilização em procedimento disciplinar de gravações que integram processo criminal, o que o TEDH aceitou no Acórdão Versini-Campinchi and Crasnianski v. França, 16 de junho de 2016, queixa n.º 49176/11, considerando que a transcrição de conversa entre o queixoso (advogado) e o seu cliente assentou no facto de decorrer do mesma que ele próprio teria cometido um crime, tendo os tribunais nacionais se assegurado de que a transcrição não infringia os direitos de defesa do seu cliente.

e) Dados biométricos

Os dados biométricos – "dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos"[141] – são dados pessoais sensíveis, como previsto no artigo 9.º, n.º 1, do RGPDP, pelo que o seu tratamento tem de ser justificado em um dos títulos a que se refere o n.º 2 do mesmo artigo[142]. Nos termos da alínea b) deste n.º 2, o empregador pode tratar os mesmos quando "for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos …em matéria de legislação laboral, … na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma

[137] Parecer 2/2017 sobre o tratamento de dados no local de trabalho, cit., p. 12.
[138] Artigo 28.º, n.º 5, da Lei n.º 58/2019.
[139] Filipa Urbana Calvão, "A proteção…", cit., p. 5.
[140] Cristóbal Molina Navarrete, "Control tecnológico…", cit., p. 335.
[141] Artigo 14.º, n.º 4, do RGPDP.
[142] A aplicação de qualquer uma destas exceções do artigo 9.º, n.º 2, do RGPDP está sujeita a condições rigorosas, que exigem uma cuidada análise caso a caso.

convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados".

Neste quadro, por sentença de 12 de agosto de 2019, o Tribunal de Amesterdão, considerando a exceção introduzida pela lei de execução do RGPD (ao abrigo da alínea b) do n.º 2 do artigo 9.º), que prevê o tratamento de dados biométricos para fins de autenticação ou segurança, relativamente à utilização de um sistema de autorização biométrica (impressão digital) para o acesso ao dinheiro pelos trabalhadores de uma sapataria, concluiu que o interesse da empresa (evitar a fraude e o roubo por parte dos trabalhadores) não era, no caso, suficiente para o tratamento dos dados biométricos se subsumir à previsão normativa nacional, que o mesmo não era proporcional, uma vez que não existiam outras medidas de segurança no estabelecimento, como alarmes de entrada/saída e videovigilância e que o empregador não demonstrou suficientemente por que razão não foram considerados outros sistemas menos invasivos da privacidade, por exemplo, uma combinação de um cartão de acesso e um código pessoal[143]. As ponderações do tribunal são consonantes com o disposto na Recomendação CM/Rec(2015) 5, citada. De acordo com esta, "[a] recolha e o tratamento posterior dos dados biométricos só deve ser efetuado quando for necessário proteger os interesses legítimos dos empregadores, trabalhadores ou terceiros, se não existirem outros meios menos intrusivos e se for acompanhado das salvaguardas adequadas…". Entre estas, destaca-se a fiabilidade científica dos métodos utilizados, a observância de requisitos de segurança, a prestação de informação clara e bastante aos trabalhadores sobre os termos da recolha e tratamento da respetiva informação e a consulta a estruturas representativas dos trabalhadores (18. e 21.).

No caso português, o artigo 28.º, n.º 6, da Lei n.º 58/2019, estabelece que os dados biométricos só podem ser tratados "para controlo de assiduidade e para controlo de acessos às instalações do empregador, devendo assegurar-se que apenas se utilizem representações dos dados biométricos e que o respetivo processo de recolha não permita a reversibilidade dos referidos dados". A norma circunscreve a utilização de tais dados face ao disposto no artigo 18.º do Código do Trabalho, que não estabelece particulares finalidades para essa utilização, enunciando apenas que o tratamento "é permitido se os dados a utilizar forem necessários, adequados e proporcionais aos objetivos a atingir". Salvaguarda, no entanto, especificamente a realização de prévia consulta à comissão de trabalhadores. Não obstante a aparente clareza da lei, enquanto título de legitimidade para a utilização de dados biométricos, é importante que tal possibilidade seja explicitada no contrato ou aquando da admissão, assim como os termos de tratamento da correspondente informação[144].

[143] Sobre este caso (7728204 CV VERZ 19-9686 – https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:6005), ver Tim Van Canneyt, "The use of biometric data in an employment context", 14.11.2019. Disponível na internet: https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/the-use-of-biometric-data-in-an-employment-context.

[144] Embora reportado ao quadro jurídico australiano, ver as dificuldades que o sistema biométrico de controlo da assiduidade pode suscitar o caso, designadamente quando introduzida após a celebração do contrato, quando não integrava os "termos e condições" deste -***Lee v Superior Wood Pty Ltd*** [2019] FWCFB 95, decidido em 1 de julho de 2019 pela *Fair Work Commission*, funcionando em pleno (disponível na internet: <URL: https://www.fwc.gov.au/documents/decisionssigned/html/2019fwcfb2946.htm).

3.3. Tratamento de dados pessoais e a cessação da relação laboral

A informação factual tornada disponível pelo tratamento de dados pessoais[145] pode ser relevante para efeitos de cessação da relação laboral (como seja, por exemplo, a informação sobre a perda de qualificação profissional pelo trabalhador, o atingir de idade determinante para reforma ou aposentação, a verificação anual pelo empregador do certificado de registo criminal do trabalhador que trabalha com crianças[146]). O artigo 88.º (tratamento de dados no contexto laboral) do RGPDP menciona, *inter alia*, a cessação da relação de trabalho como um domínio onde se podem justificar "normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores" (n.º 1), prevendo medidas que acautelem a respetiva dignidade, interesses legítimos e direitos fundamentais, "com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho" (n.º 2).

Como situação relevante no plano da transferência de dados pessoais e da necessidade de prestação clara ao trabalhador pode nomear-se a previsão, no artigo 176.º, n.º 5, da LTFP, da continuação do procedimento disciplinar e da execução da sanção disciplinar, consoante os casos, suspensos por força da cessação da relação de emprego público, se o trabalhador vier no período de 18 meses a constituir uma nova relação de emprego para o exercício das "mesmas funções". Uma das questões que se coloca é a de saber se, no caso da constituição de uma nova elação jurídica com um empregador diferente, este tem – se e quando tomar conhecimento da situação disciplinar pendente –, comunicar ao empregador anterior a nova situação e se, retomando-se a anterior relação jurídica, ainda que temporariamente, ela pode coexistir com a nova relação de emprego. Na verdade, a referência a "mesmas relações jurídicas" parece apontar para que a norma não seja operável na economia de uma relação jurídica com um novo empregador. O princípio da transparência é, em qualquer caso, determinante, ou seja, tem de ser prestada ao trabalhador informação clara e completa sobre o alcance da nova admissão.

Independentemente destas normas e de normas específicas esclarecedoras ou autorizativas do tratamento de dados, os princípios têm um papel decisivo, como já destacado. Assim, por exemplo, princípio da exatidão (artigo 5.º, n.º 1, alínea d), do RGPDP) implica registos precisos sobre a iniciativa e o motivo da cessação da relação jurídica e sobre a informação transmitida

[145] Recorde-se que tratamento de dados pessoais constitui "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 utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, …" (artigo 4.º, n.º 2, do RGPDP).

[146] Neste contexto, tenha-se presente que o registo criminal pode relevar em sede de admissão a emprego, assim como importar a sua modificação ou extinção. É o que resulta, por exemplo, do disposto no n.ºs 1 e 2 do artigo 2.º ("medidas de prevenção de contacto profissional com menores") da Lei n.º 113/2009, de 17.12, que estabelece medidas de proteção de menores, em cumprimento do artigo 5.º da Convenção do Conselho da Europa contra a Exploração Sexual e o Abuso Sexual de Crianças, e procede à segunda alteração à Lei n.º 57/98, de 18.08, considerada na versão atualizada). O empregador está obrigado "a pedir ao candidato a apresentação de certificado de registo criminal e a ponderar a informação constante do certificado na aferição da idoneidade do candidato para o exercício das funções" quando esteja em causa o "recrutamento para profissões, empregos, funções ou atividades, públicas ou privadas, ainda que não remuneradas, cujo exercício envolva contacto regular com menores" (n.º 1). Do mesmo modo, deve anualmente, após o recrutamento, ponderar a informação constante do mesmo [registo criminal] na aferição da idoneidade para o exercício das funções" (n.º 2), sob pena de incorrer em responsabilidade contraordenacional ou mesmo criminal (n.ºs 8, 9, 13 e 14).

ao trabalhador sobre as razões da cessação[147]. O princípio da limitação da conservação (artigo 5.º, n.º 1, alínea e), do RGPDP) importa a existência de prazos para a retenção de dados pessoais, os quais, *inter alia*, devem ponderar o facto de os empregadores e os trabalhadores poderem necessitar destes dados "por razões jurídicas, a fim de fornecerem provas sobre qualquer questão relativa a uma relação de trabalho anterior ou atual"[148].

No caso Garamukanwa v. Reino Unido (Acórdão do TEDH de 14.05.2019, queixa n.º 70573/17), Garamukanwa queixou-se, por referência ao artigo 8.º da Convenção, de que a decisão do *National Health Service Trust* de o despedir do seu emprego se baseava em informação privada, "incluindo o material do iPhone e correio eletrónico pessoal e a correspondência Whatsapp entre ele e a L.M.", que o empregador não tinha o direito de utilizar e, bem assim, que "não tinha o direito de conservar ou invocar as provas que lhe foram fornecidas pela polícia" (n.º 18). O *National Health Service Trust* despediu, após procedimento disciplinar, o queixoso em dezembro de 2013 por falta grave, tendo-se baseado, nomeadamente, "em fotografias guardadas no seu iPhone, transmitidas pela polícia, ligando-as a determinadas mensagens de correio eletrónico anónimas, bem como a mensagens pessoais e mensagens WhatsApp trocadas pelo queixoso e outros trabalhadores, incluindo a L.M." O queixoso fora advertido pelo empregador quando ao carácter inapropriado da sua conduta cerca de um ano antes do início das investigações pela polícia, e, durante o mesmo procedimento, forneceu voluntariamente algumas das comunicações No caso, o TEDH destacou, assim, que o queixoso "não podia razoavelmente esperar que quaisquer materiais ou comunicações que estivessem relacionados com as alegações feitas pela L.M. permanecessem privados" (n.º 27)[149]. No caso, sobressai o contexto laboral em que as comunicações tiveram lugar (n.º 25). É ainda sublinhada "a importância de as entidades patronais interpelarem um trabalhador desde uma fase inicial das alegações de má conduta que lhe são imputadas"[150].

[147] O artigo 341.º do Código do Trabalho e o artigo 290, n.ºs 1 e 2, da LTFP determinam que o certificado de trabalho, a emitir pelo empregador com a cessação do contrato, para além das "datas de admissão e de cessação" e do "cargo ou cargos desempenhados", só deve conter outras "referências" que forem pedidas pelo trabalhador.

[148] *Protección de los datos personales de los trabajadores*, Organización Internacional del Trabajo 1997, Primera edición 1997, n.º 8.5., alínea c). Ver, igualmente, os artigos 17.º, n.º 3, alínea e), 18.º, n.º 1, alínea c), e n.º 2, e 21.º, n.º 1, parte final, do RGPDP.

O artigo 46.º da Lei n.º 102/2009, de 10.09 (regime jurídico da promoção da segurança e saúde no trabalho), estabelece que "o empregador deve organizar e conservar arquivos atualizados, nomeadamente por via eletrónica" sobre determinados dados relativos à exposição a riscos e à vigilância da saúde dos trabalhadores (n.º 1), pelo período de 40 anos (n.º 2).

No caso de a empresa ou serviço cessar a atividade, "os registos e arquivos devem ser transferidos para o organismo competente do membro do Governo responsável pela área laboral, com exceção das fichas clínicas, que devem ser enviadas para o organismo competente do ministério responsável pela área da saúde, os quais asseguram a sua confidencialidade" (n.º 4).

[149] "La información proporcionada por estos utillajes puede ser utilizada como medio de prueba para acreditar comportamientos irregulares justificativos de una separación del servicio, de un despido o de otro tipo de sanciones, consecuencias favorecidas por la generalizada ambigüedad de las relaciones de puestos de trabajo, la falta de reglas claras sobre asignación de tareas y la carencia de formación en técnicas de liderazgo." Susana Rodríguez Escanciano, "Posibilidades…", cit., p. 112.

[150] Joanne Frew, "Can using material found on an employee's phone in criminal proceedings be used as evidence for an internal disciplinary process?", 28.6.2019. Disponível na internet: <URL: https://www.dwf.law/Legal-Insights/2019/June/Using-employee-phone-in-criminal-proceedings. Como destacam Michelle Hobbs e Shaun Hogan, no caso Garamukanwa, a fonte e os destinatários das comunicações foram relevantes, tal como o conteúdo das comunicações e o facto de as comunicações não serem de natureza puramente pessoal, contudo, o fator determinante foi o facto de o trabalhador ter sido efetivamente avisado pelo seu empregador de que o seu comportamento era inadequado. "Disciplinaries and the right to privacy". Disponível na internet in: <URL https://www.stevens-bolton.com/site/insights/articles/disciplinaries-and-the-right-to-privacy.

O *Employment Appeal Tribunal*, no Reino Unido, no caso ***Phoenix House Ltd v. Mrs Tatiana Stockman*** UKEAT/0058/18/OO, de 5 de julho de 2019, relativizou a utilização por trabalhador objeto despedimento ilícito de gravação de reunião no departamento de recursos humanos, destacando, entre o mais, a falta de previsão como infração disciplinar da realização de uma tal gravação, o facto de a gravação ser permitida por qualquer dispositivo móvel sem um sentido específico e o propósito altamente relevante da gravação[151].

4. Comunicação a outrem de dados pessoais dos trabalhadores

4.1. A comunicação a outrem de dados pessoais dos trabalhadores como uma operação de tratamento

A comunicação ou a transmissão a outrem de dados pessoais dos trabalhadores constitui uma operação de tratamento de dados (artigo 4.º, n.º 1, alínea c), do RGPDP)[152] e, como tal, pode ocorrer se existir um título jurídico para o efeito (*v.g.*, artigos 5.º, n.º 1, alínea a), 6.º e 9.º do RGPDP). Pode igualmente constituir uma decorrência da finalidade que justificou o seu tratamento originário (artigo 5.º, n.º 1, alínea b), do RGPDP[153]), como seja, por exemplo, a colocação à disposição da autoridade nacional com competência para a fiscalização das condições de trabalho do registo dos tempos de trabalho[154].

São vários os títulos jurídicos que podem enquadrar a comunicação a terceiros de dados sobre os trabalhadores. Consideremos alguns destes títulos.

a) O cumprimento de obrigações do empregador que relevam para o cumprimento de aspetos essenciais da legislação do trabalho[155].
Mencione-se, por exemplo, a obrigação de o empregador enviar informação anual "sobre a atividade social da empresa" – designadamente quanto a "remunerações, duração do trabalho, trabalho suplementar, contratação a termo, formação profissional, segurança e saúde no trabalho e quadro de pessoal" – ao, por um lado, "serviço com competência inspetiva do ministério responsável pela área laboral" e, por outro lado, aos "sindicatos representativos de trabalhadores da empresa que a solicitem", à comissão de trabalhadores, bem como aos "representantes dos trabalhadores para a segurança e saúde no trabalho na parte relativa às matérias da sua competência" e às "associações de empregadores representadas na Comissão Permanente de Concertação Social que a solicitem" (artigo 6.º, n.º 1, alínea c), e artigo

[151] Sobre este caso, ver Nicholas Robertson, United Kingdom, The Labour and Employment Dispute Review, March 2020. [Consul. 28 abr. 2020]. Disponível na internet: <URL: https://thelawreviews.co.uk/edition/the-labour-and-employment-disputes-review-%E2%80%93-edition-3/1215996/united-kingdom. A Decisão está disponível in: <URL: https://www.gov.uk/employment-appeal-tribunal-decisions/phoenix-house-limited-v-mrs-tatiana-stockman-ukeat-0058-18-oo.

[152] Igualmente salientando este aspeto ver, *v.g.*, Acórdão do TJUE de 20.07.2016, Athanassios Oikonomopoulos contra Comissão Europeia**,** T-483/13, n.º 53.

[153] Recomendação Rec(2015)5, citada, 8.2., alínea i).

[154] Acórdão de 30.05.2013, C-342/12, Worten - Equipamentos para o Lar, SA contra Autoridade para as Condições de Trabalho.

[155] *V.g.*, Recomendação Rec(2015)5, 8.2., alínea iii), na qual consta a transmissão de informação "se a comunicação estiver prevista na legislação nacional e, em especial, quando necessária para o cumprimento de obrigações legais ou em conformidade com acordos coletivos".

9.º, n.º 2, alínea b), do RGPDP; artigo 32.º da Lei 105/2009, de 14.09, e Portaria n.º 55/2010, de 21.01[156]).

A informação a prestar é nominal, dada a relevância factual da informação para a valia do controlo inerente à atividade social da empresa. No entanto, por força de alteração resultante da Lei n.º 60/2018, de 21.08, a informação prestada aos sindicatos e comissão de trabalhadores não é nominativa (salvo quanto ao sexo e quanto às remunerações) quando seja transmitida aos sindicatos (artigo 32.º, n.º 8). De igual modo, não é nominativa quando transmitida ao serviço competente para tratamento estatístico (artigo 89.º do RGPDP[157]).

Na verdade, o controlo do cumprimento de normas tão importantes como as relativas à contratação a termo, à discriminação no trabalho e no emprego, à tutela da parentalidade não deve precludir o acesso a informação nominativa funcional pertinente para efeito, por exemplo, do exercício do direito de ação em representação ou apoio dos trabalhadores, designadamente ao abrigo do artigo 9.º da Diretiva 2000/78/CE, que estabelece um quadro geral de igualdade de tratamento no emprego e na atividade profissional. Em termos gerais, por exemplo, o artigo 443.º, n.º 1, alínea d), do Código do Trabalho prevê o direito das associações sindicais "[i]niciar e intervir em processos judiciais e em procedimentos administrativos quanto a interesses dos seus associados, nos termos da lei". Ora, os representantes dos trabalhadores têm de "receber os dados pessoais dos trabalhadores na medida em que tal seja necessário para lhes permitir representar os interesses dos trabalhadores ou se esses dados forem necessários para cumprir ou supervisionar as obrigações previstas nos acordos coletivos"[158].

b) A comunicação de dados pessoais pode funda-se no exercício de direitos e interesses tuteláveis de outrem[159]. É o caso do exercício do direito à informação e do direito de acesso aos arquivos e registos administrativos (artigo 268.º, n.os 1 e 2, da CRP)[160] e do direito à tutela jurisdicional efetiva (artigo 268.º, n.os 4 e 5, da CRP; e *v.g.*, artigo 78.º-A, n.º 1[161], do Código de Processo nos Tribunais Administrativos[162].

---

[156] Regula o conteúdo do relatório anual referente à informação sobre a atividade social da empresa e o prazo da sua apresentação, por parte do empregador, ao serviço com competência inspetiva do ministério responsável pela área laboral.

[157] Nos termos do artigo 5.º, n.º 1, alínea b), do RGPDP, o tratamento posterior de dados pessoais "para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1".

[158] *Handbook on European data protection law*, cit., p. 334.

[159] O artigo 6.º, n.º 1, alínea f), do RGPDP prevê o tratamento de dados pessoais necessário para efeito dos interesses legítimos, quer do responsável pelo tratamento, quer por terceiros, sem prejuízo da ponderação da eventual prevalência dos "interesses ou direitos e liberdades fundamentais do titular" que exijam em concreto a mesma. O artigo 9.º, n.º 2, alínea f), refere-se ao tratamento "necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional".

[160] O *UK Data Protection Act 2018* (http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) prevê, especificamente:

> "It is an offence for a person listed in subsection (4) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive." (cfr. 173 [Alteration etc of personal data to prevent disclosure to data subject] (3))

[161] "Quando o autor não conheça, no todo ou em parte, a identidade e residência dos contrainteressados, pode requerer à Administração, previamente à propositura da ação, a passagem de certidão da qual constem aqueles elementos de identificação".

[162] Lei n.º 15/2002, de 15.02, considerada na versão atualizada.

Pode também ser o caso igualmente o caso do "direito a condições de trabalho saudáveis, seguras e dignas"[163]: no Acórdão de 13.07.2018, SQ v. Banco Central Europeu de Investimentos, T-377/17, o Tribunal Geral da União Europeia considerou que aquele direito foi violado, concretamente, a saúde e a dignidade do trabalhador, pela decisão do presidente do Banco que impôs "ao destinatário dessa decisão uma obrigação de confidencialidade contrária aos objetivos de um processo de inquérito relativo a um caso alegado de assédio moral"[164]. No caso, o Tribunal Geral destacou ainda que "[e]sta ilegalidade, que afeta a decisão impugnada, impôs um período de silêncio indevido à recorrente, pelo que essa proibição de falar sobre esse assunto lhe causou um prejuízo moral que não pode ser integralmente reparado por meio da simples anulação da decisão impugnada"[165].

c) A comunicação de dados pessoais a terceiros tem igualmente lugar por forca do "exercício de funções de interesse público", como acontece, por exemplo, quando um serviço inspetivo, de auditoria e controlo dá a conhecer a outras entidades públicas ou dá pública notícia dos relatórios e demais documentos, que incluem dados pessoais (como, por exemplo, o nome dos administradores das empresas fiscalizadas) que não podem ser suprimidos sem prejuízo para o fim que têm de cumprir[166].

d) Tratando-se de trabalhadores do sector público, a comunicação de dados pessoais pode fundar-se, especificamente, nas exigências de transparência, "incluindo o controlo da correta utilização dos recursos e fundos públicos", sem prejuízo das salvaguardas decorrentes do RGPDP atinentes, designadamente aos princípios da finalidade, da minimização e da transparência, e, bem assim, do direito do trabalhador à privacidade[167] (8.3.).

A publicidade e comunicação a terceiros à relação jurídica de dados pessoais dos titulares de órgãos e agentes administrativos e agentes públicos em geral – relevantes para a tutela dos interesses públicos referidos e, bem assim, para a tutela dos direitos e interesses de terceiros – está prevista em vários passos do RGPDP. De acordo com o § 154 do preâmbulo do Regulamento (UE) n.º 2016/679, "[o] acesso do público aos documentos oficiais pode ser considerado de interesse público. Os dados pessoais que constem de documentos na posse dessas autoridades públicas ou organismos públicos deverão poder ser divulgados publicamente por tais autoridades ou organismos, se a divulgação estiver prevista no direito da União ou do Estado-Membro que lhes for aplicável". O artigo 86.º concretiza que "[o]s dados pessoais que constem de documentos oficiais na posse de uma autoridade pública ou de um organismo público ou privado para a prossecução de atribuições de interesse público podem ser divulgados pela autoridade ou organismo nos termos do direito da União ou do Estado-Membro que for aplicável à autoridade ou organismo público, a fim de conciliar o acesso do público a documentos oficiais com o direito à proteção dos dados pessoais nos termos do … regulamento". É o caso, por exemplo, da publicidade dos

[163] Artigo 31.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia.
[164] Cfr. n.º 158.
[165] Cfr. n.º 184.
[166] Acórdão do TJUE de 20.07.2016, Athanassios Oikonomopoulos contra Comissão Europeia, T-483/13, n.ºs 60-93. A Recomendação Rec(2015)5, citada, estabelece que os dados pessoais recolhidos para efeitos de emprego só devem ser comunicados a entidades públicas no domínio e para efeitos do exercício das suas funções, nos "limites das obrigações legais dos empregadores ou em conformidade com outras disposições de direito interno" (8.1.).
[167] Ver 8.3. da Recomendação Rec(2015)5.

rendimentos e património dos que exercem cargos públicos, assim como dos seus dados curriculares[168], mas igualmente da publicação de atos em matéria de pessoal pelas entidades públicas que envolvam encargos públicos[169].

e) Em termos gerais, seja qual for o setor em que se insiram e a área de atividade, releva a divulgação e publicidade de dados pessoais no contexto do exercício da "liberdade de expressão e de informação, incluindo o tratamento para fins jornalísticos e para fins de expressão académica, artística ou literária" (artigo 85.º do RGPD), como já destacado.

Há que cumprir, em particular, obrigações de publicidade decorrentes de diplomas específicos, como a Diretiva 2003/98/CE do Parlamento Europeu e do Conselho, de 17 de novembro de 2003, relativa à reutilização de informações do setor público[170] (que será substituída pela Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informações do setor público com efeitos a partir de 17 de julho de 2021 – artigo 19.º) e o Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo aos requisitos prudenciais para as instituições de crédito e para as empresas de investimento e que altera o Regulamento (UE) n.º 648/2012[171].

Os dados comunicados pelos empregadores devem ser, de acordo com os princípios da finalidade e da minimização, os "dados relevantes, exatos e atualizados", o que é "especialmente em relação aos dados que são colocados em linha e acessíveis a um público mais vasto"[172], sendo passível de gerar responsabilidade a comunicação de dados inexatos, imprecisos e incompletos[173].

---

[168] O TEDH concluiu, no Acórdão de 26.03.2020, Centre for Democracy and the Rule of Law v. Ukraine, queixa n.º 10090/16, de forma unânime, que houve violação da liberdade de expressão do Centre for Democracy and the Rule of Law (artigo 10.º da Convenção Europeia dos Direitos do Homem), em virtude da decisão de recusar à organização o acesso a informação sobre a educação e o historial profissional dos líderes políticos (candidatos a cargos eletivos) contidas nos seus currículos.
No Acórdão n.º 20/2019, de 23 de janeiro de 2019, o TC italiano analisou a publicação *online* do rendimento e património de todos os dirigentes da Administração Pública, dos seus cônjuges e parentes até ao segundo grau. O TC considerou excessiva a abrangência subjetiva da obrigação de publicidade a cargos dirigentes de menor relevância, diferentemente, desde logo, daqueles com "tarefas - proactivas, organizacionais, de gestão (de recursos humanos e instrumentais) e de despesas - da maior importância…". (n.º 6).

[169] Ver, por exemplo, artigos 4.º e 5.º da Lei n.º 35/2014, de 22.06, que aprova o Código do Trabalho; artigos 12.º e 18.º do Decreto-Lei n.º 11/2012, de 20.01, que estabelece a natureza, a composição, a orgânica e o regime jurídico a que estão sujeitos os gabinetes dos membros do Governo.

[170] FÉ revogada pela Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informações do setor público com efeitos a partir de 17 de julho de 2021 (artigo 19.º).

[171] No Acórdão de 14.11.2018, C-215/17, Nova Kreditna Banka Maribor d.d. contra Republika Slovenija, o TJUE concluiu: "O artigo 1.º, n.º 2, alínea c), terceiro travessão, da Diretiva 2003/98/CE do Parlamento Europeu e do Conselho, de 17 de novembro de 2003, relativa à reutilização de informações do setor público, e o artigo 432.º, n.º 2, do Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo aos requisitos prudenciais para as instituições de crédito e para as empresas de investimento e que altera o Regulamento (UE) n.º 648/2012, devem ser interpretados no sentido de que não se aplicam a uma legislação nacional, como a que está em causa no processo principal, que impõe a um banco que esteve sob a influência dominante de uma entidade de direito público a divulgação dos dados relativos aos contratos para a prestação de serviços de consultoria, advocacia, de direitos de autor e de outros serviços de natureza intelectual, celebrados pelo referido banco no período em que esteve sob essa influência dominante, sem admitir nenhuma exceção a tal obrigação a título da preservação do segredo comercial desse banco e, por conseguinte, não se opõem a essa legislação nacional."

[172] Artigo 5.º, n.º 1, alínea c), do RGPDP; e Recomendação Rec(2015)5, 8.4.

[173] *V.g.*, artigo 485.º e artigo 573.º do Código Civil e artigo 11.º, n.º 2, do CPA.

4.2. A comunicação de dados pessoais a outrem e o direito de portabilidade dos dados

A comunicação a terceiros pelo empregador de dados pessoais do trabalhador pode ser do interesse do trabalhador. Neste caso, pode ter lugar com base no "consentimento expresso, livre e informado do trabalhador em causa"[174] e pode resultar do exercício do direito de portabilidade dos dados, que integra o direito de os comunicar a terceiros. Com efeito, o direito de portabilidade dos mesmos importa no contexto laboral: *i)* o direito do trabalhador receber os dados pessoais que lhe digam respeito e que tenha fornecido ao empregador ou a outrem por conta do empregador[175], "num formato estruturado, de uso corrente e de leitura automática"; *ii)* "o direito de transmitir esses dados a outro responsável pelo tratamento", sem que o empregador ou subcontratante deste, "a quem os dados pessoais foram fornecidos o possa impedir" se o tratamento dos dados se basear num contrato, no consentimento ou se "for realizado por meios automatizados" (artigo 20.º, n.º 1, do RGPDP); *iii)* e o direito a que, nesse caso, "sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível" (artigo 20.º, n.º 2, do RGPDP). A inclusão em suportes informáticos dos dados dos trabalhadores facilita o seu tratamento e, neste caso, o cumprimento das pretensões dos trabalhadores relativamente aos mesmos, designadamente no exercício do direito de portabilidade dos seus dados[176].

5. Direitos dos trabalhadores decorrentes do regime de proteção de dados pessoais

São vários os direitos dos trabalhadores decorrentes do RGPDP, direitos cujo exercício o empregador deve facilitar[177]. Entre estes direitos, destaca-se o direito de o trabalhador ser informado sobre as operações de tratamento dos seus dados e sobre as respetivas finalidades[178], incluindo sobre os termos do controlo da atividade laboral mesmo que este "seja lícito e proporcional"[179]. A informação deve ser clara, precisa e oportuna[180].

Os trabalhadores têm, relativamente aos dados pessoais de que o empregador disponha sobre si, o direito de aceder aos mesmos[181] (incluindo quando se apresentem sob a forma de áudio e vídeo[182]) e o direito de obter sem demora a retificação dos dados inexatos e a que sejam completados os dados incompletos[183]. Têm igualmente o direito ao apagamento dos dados quando "deixarem de ser necessários para a finalidade que motivou a sua recolha ou tratamento" e quando possa opor-se ao seu tratamento "por motivos relacionados com a sua

[174] Recomendação Rec(2015)5, 8.2., alínea b).
[175] Constitui subcontratante "uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes" (artigo 4.º, n.º 7), do RGPDP).
[176] Susana Rodríguez Escanciano ("Posibilidades…", cit., p. 111) destaca que a "gestão informatizada do pessoal significa que todos os dados relativos ao desenvolvimento do vínculo de funcionário ou da relação de trabalho, desde o momento do recrutamento, passando pelo desenvolvimento das tarefas profissionais, até à sua conclusão, facilita a sua inclusão em suportes informáticos capazes de unificar instantaneamente e de forma devidamente atualizada dados dispersos".
[177] Artigo 12.º, n.º 2, do RGPDP.
[178] *V.g.*, artigo 12.º, n.º 1, e artigos 13.º e 14.º do RGPD.
[179] Jaime Cabeza Pereiro, *"El necesario cambio en la jurisprudencia constitucional sobre videovigilacia y control", Temas Laborales*, núm. 141/2018, p. 23 (pp. 13-36).
[180] *V.g.*, Jaime Cabeza Pereiro, *"El necesario cambio…", cit.*, p. 31; e artigo 12.º do RGPDP.
[181] Artigo 15.º do RGPD.
[182] Acórdão do TEDH de 17 de outubro de 2019, López Ribalda, cit., n.º 154.
[183] Artigos 16.º e 18.º, n.º 1, alínea a), do RGPD.

situação particular", sem que "existem interesses legítimos prevalecentes que justifiquem o tratamento". O direito cede, no entanto, na medida necessária, quando importe salvaguardar, entre outras motivos, "o cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento", o "exercício da liberdade de expressão e de informação" e a "declaração, exercício ou defesa de um direito num processo judicial"[184].

Se as regras de tratamento dos dados não forem observadas e, especificamente, se o exercício de algum dos direitos que o trabalhador tem na economia do RGPDP for recusado ou não for assegurado, a legislação nacional deve prever meios de tutela adequados para o efeito, que compreendem necessariamente o "direito à ação judicial"[185], a qual pode ser desencadeada por organização estatutariamente habilitada (como as associações sindicais), atuando em representação do trabalhador[186]. Note-se que, não acautelando o empregador o exercício dos direitos do trabalhadores, deve informar o mesmo, "sem demora e, o mais tardar, no prazo de um mês a contar da data de receção do pedido", não só "das razões que o levaram a não tomar medidas", como "da possibilidade de apresentar reclamação a uma autoridade de controlo" e de "intentar ação judicial"[187].

No Acórdão de 17 de outubro de 2019, López Ribalda, citado, relativamente à utilização de tecnologias de informação e de comunicação, o TEDH sublinhou que os trabalhadores devem "ter acesso a um recurso perante um órgão judicial independente com jurisdição para determinar, pelo menos em substância, se as condições relevantes foram cumpridas" (n.º 118). No que se refere à utilização de "gravações de videovigilância", esclareceu que "deve ser examinado se o requerente teve oportunidade de contestar a autenticidade das provas e de se opor à sua utilização"; e, bem assim, ser tido em conta "a qualidade da prova" e se as "circunstâncias em que foi obtida lançam dúvidas sobre sua confiabilidade ou precisão". Referiu, ainda, que, embora "nenhum problema de justiça surja necessariamente quando a prova obtida não foi apoiada por outro material", quando a mesma "é muito forte e não há risco de não ser confiável, a necessidade de prova de apoio é correspondentemente menor" (n.º 151).

6. Notas finais

O regime jurídico de proteção de dados pessoais - constante, no essencial, do Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 -, como noutros domínios da vida dos indivíduos, reforça a posição jurídica dos trabalhadores nas relações laborais, assim como dos candidatos aos empregos[188].

[184] Artigo 17.º do RGPDP.
[185] Artigo 79.º do RGPDP.
[186] Artigo 80.º do RGPDP.
[187] Artigo 12.º, n.º 4, do RGPDP.
[188] No Plano de Ação da UE para os Direitos Humanos e a Democracia no período 2020-2024 JOIN/2020/5 final, de 25.3.2020, Comunicação da Comissão Europeia conjunta ao Parlamento Europeu e ao Conselho, no ponto sobre a "independência e o pluralismo dos meios de comunicação social, o acesso à informação e a luta contra a desinformação" (C.), o destaque primeiro vai para a necessidade de "[a]poiar as iniciativas legislativas sobre o

O RGPDP consolida a separação entre a esfera de proteção do direito à proteção de dados face à esfera de proteção do direito à reserva da vida privada, tornando clara a maior amplitude e a distinção qualitativa daquela face à deste, afirmando-se como "uma liberdade positiva de controlo e intervenção" dos indivíduos em relação aos seus próprios dados[189], que se consubstancia numa séria de direitos procedimentais oponíveis aos responsáveis pelo seu tratamento e, portanto, invocáveis pelos trabalhadores em face do empregador. Independentemente desta invocação, o empregador tem o dever de adotar "medidas técnicas e organizativas adequadas" à garantia dos "princípios da proteção de dados", tais como os da transparência, da minimização dos dados, da exatidão e da integridade de dados e à proteção dos "direitos dos titulares dos dados"[190].

O RGPDP afirma-se como um diploma de defesa dos direitos e liberdades fundamentais, seja das liberdades pessoais, seja das liberdades fundamentais do mercado interno[191]. O direito à proteção dos dados pessoais, à luz RGPDP, favorece a liberdade de expressão e de informação dos trabalhadores – cujo exercício pode ser prejudicado, seja pelo acesso indevido do empregador a dados pessoais funcionalmente irrelevante[192], seja pela restrição de informação que releva para tal exercício[193] –; favorece a separação entre a esfera profissional e a esfera pessoal de vida do trabalhador; favorece a aplicação do direito à não discriminação.

Em 23 de abril de 2020, o responsável máximo pelo Comité Europeu para a Proteção de Dados, em resposta a questão colocada por deputada europeia relativa à necessidade de orientações comuns sobre a aplicação do Regulamento Geral sobre a Proteção de Dados e de outros instrumentos jurídicos relevantes da UE em matéria de proteção de dados na luta contra a pandemia da COVID-19, respondeu que o regime existente era suficiente, que assegurar a transparência, a qualidade dos dados e a confiança é fundamental para o cumprimento do quadro jurídico da UE em matéria de proteção de dados pessoais[194]. Sintetizou, desta forma, o essencial desta proteção e é a esta luz que deve ser vista nas relações laborais, que devem ser relações de confiança e certeza jurídicas para as respetivas partes e, particularmente, de respeito pelo direito do trabalhador a dispor da sua pessoa, da sua esfera de autodeterminação pessoal[195], mas igualmente de respeito pela sua dignidade enquanto trabalhador sem a qual perde sentido a própria relação laboral[196].

---

acesso à informação, o direito à privacidade e à proteção dos dados pessoais, em conformidade com as normas europeias e internacionais, bem como a sua aplicação efetiva".

[189] C. OGRISEG, "GDPR and Personal Data Protection in the Employment Context", cit., p. R. 8.

[190] Artigos 25.º, 5.º e 16.º a 22.º do RGPDP.

[191] Artigo 1.º, n.ºs 2 e 3, do RGPDP.

[192] Acórdão do TEDH de 06.11.2012, Redfearn v. the United Kingdom, queixa n.º 47335/06. A consideração da filiação partidária determinou, no caso, o despedimento de trabalhador.

[193] Recorde-se que no caso do Acórdão Sergejs Buivids, C-345/17, n.º 69, o TJUE esclareceu que "[o] artigo 9.° da Diretiva 95/46 [artigo 85.º, n.º 1*, do RPDP] deve ser interpretado no sentido de que circunstâncias de facto como as do litígio no processo principal, a saber, a gravação vídeo de agentes da polícia numa esquadra, aquando de uma prestação de declarações, e a publicação do vídeo assim gravado num sítio Internet de vídeos no qual os utilizadores podem carregar, visualizar e partilhar os mesmos, podem constituir um tratamento de dados pessoais para fins exclusivamente jornalísticos…, desde que resulte do referido vídeo que a referida gravação e a referida publicação têm por única finalidade a divulgação ao público de informações, opiniões ou ideias, o que incumbe ao órgão jurisdicional de reenvio verificar".

[194] "…maintaining transparency, data quality and trust is key for complying with the EU legal framework on data protection" – carta com a referência Ref: OUT2020-0030.

[195] José Luis Monereo Pérez y Pompeyo Gabriel Ortega Lozano, "Prohibición de discriminación", *Temas Laborales*, núm. 145/2018, p. 367 ("…la subordinación jurídico-organizativa del trabajador no debe suponer la mercantilización

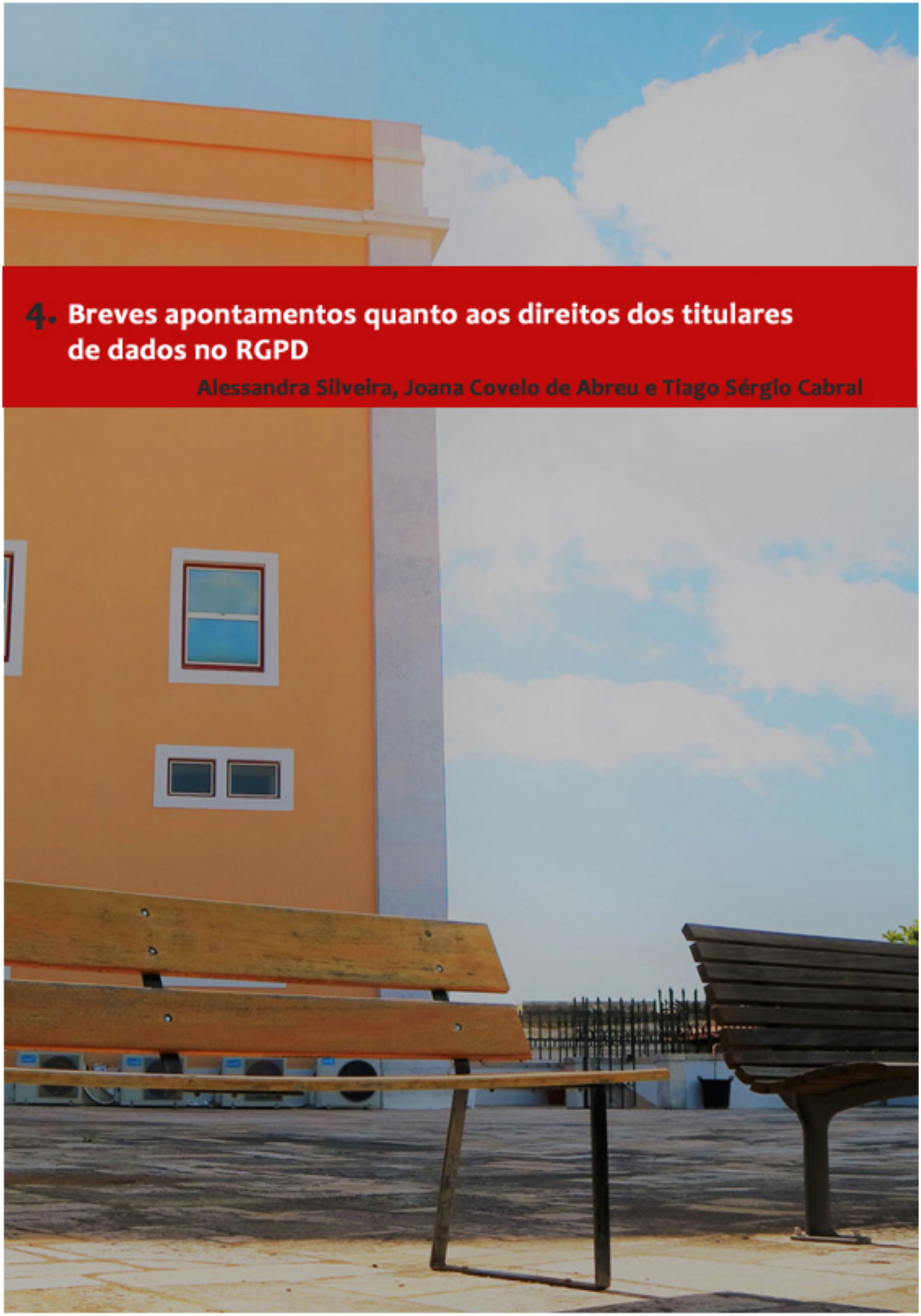
Vídeo da apresentação

https://educast.fccn.pt/vod/clips/ey9r3rqxo/ipod.m4v?locale=pt

o la privación de su consideración como sujeto libre o el desconocimiento de los aspectos que permiten el libre desarrollo de su personalidade.").

[196] Recorde-se que o artigo 31.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia consagra o direito de todos os trabalhadores a "condições de trabalho saudáveis, seguras e dignas". E, bem assim, a orientação da introdução de normas específicas relativamente ao tratamento de dados no contexto laboral para a proteção da "dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados" (n.º 2).

CENTRO
DE ESTUDOS
JUDICIÁRIOS



4. Breves apontamentos quanto aos direitos dos titulares de dados no RGPD

Alessandra Silveira, Joana Covelo de Abreu e Tiago Sérgio Cabral

CENTRO
DE ESTUDOS
JUDICIÁRIOS

4. BREVES APONTAMENTOS QUANTO AOS DIREITOS DOS TITULARES DE DADOS NO RGPD•

Alessandra Silveira*
Joana Covelo de Abreu**
Tiago Sérgio Cabral***

1. Notas introdutórias

Sendo expectável um crescente aumento do número de litígios decorrentes da alegada violação de disposições relativas à proteção de dados de caráter pessoal, o presente texto pretende contribuir com breves apontamentos sobre os direitos dos titulares de dados pessoais constantes no Regulamento 2016/679/UE 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 (doravante, "RGPD"). Este esforço incidirá sobretudo nos artigos constantes do Capítulo III do RGPD, que correspondem aos artigos 12.º a 23.º do referido diploma, sendo abordados:

a) O Direito à Informação;
b) O Direito de Acesso;
c) O Direito à Retificação;
d) O Direito ao Apagamento;
e) O Direito à Limitação do Tratamento;
f) O Direito de Portabilidade;
g) O Direito de Oposição; e
h) O Direito a Não Ficar Sujeito a Decisões Individuais Automatizadas.

• Apresentação decorrente da ação de formação contínua do CEJ "Proteção de Dados Pessoais", realizada a 19 de junho de 2019.

* Professora da Escola de Direito da Universidade do Minho e Diretora do Mestrado em Direito da União Europeia. Titular da Cátedra Jean Monnet em Direito da União Europeia.
** Professora da Escola de Direito da Universidade do Minho e da Universidade Portucalense Infante D. Henrique. Coordenadora do Módulo *Jean Monnet eUjust* "EU Procedure and credits' claims: approaching electronic solutions under e-Justice paradigm" (2019-2022).
*** Advogado.

Por motivos relacionados com as limitações naturais de um texto que se pretende sucinto e meramente introdutório, não serão abordados outros direitos que assistem ao titular dos dados e que, certamente, podem revestir elevado interesse na aplicação prática do RGPD, como sejam *i)* o direito de apresentar reclamação *a uma* ou *contra uma* autoridade de controlo (artigos 77.º e 78.º do RGPD) ou *ii)* os direitos à ação judicial contra o responsável pelo tratamento e subcontratante e de indemnização e responsabilidade (artigos 79.º e 82.º do RGPD). Tal resulta do facto de tais direitos surgirem como instrumentais à proteção de dados pessoais, configurando-se como concretizadores da tutela administrativa e jurisdicional efetiva conferida ao seu titular – ficando, por tal razão, fora do âmbito desta contribuição. Assim, a reflexão vocacionar-se-á a *i)* expor, de forma não exaustiva, os direitos e as normas que os estatuem; e a *ii)* sublinhar circunstâncias que poderão acarretar maiores dúvidas ao intérprete, tentando-se, sempre que possível, aventar possíveis soluções.

2. Direitos dos titulares dos dados

2.1. Direito à Informação

Integrado numa lógica de maior transparência para com o titular dos dados, bem como de autodeterminação relativamente ao uso dos seus dados pessoais, o Direito à Informação pode (porventura) ser considerado como o mais importante de entre os direitos elencados no RGPD. Com efeito, sem apropriada informação, o titular dos dados muito dificilmente poderia fazer uso de todos os outros direitos facultados pelo RGPD, diminuindo sobremaneira a eficácia do diploma[1].
A informação a ser prestada deve ser concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, além de adaptada à circunstância[2] e ao destinatário[3]. A informação deverá ser fornecida de forma gratuita[4].

Por forma a evitar a fadiga informativa, os responsáveis pelo tratamento deverão ter particular atenção ao excesso de informação, bem como à informação sobre privacidade que não se

[1] Tiago Sérgio Cabral, *AI Regulation in the European Union: Democratic Trends, Current Instruments and Future Initiatives* (Dissertação de Mestrado: Universidade do Minho, 2019), 131 e ss.
[2] Por regra, a informação deverá ser prestada por escrito. No entanto, quando isto não seja possível ou adequado, pode considerar-se a utilização de outros meios complementares ou mesmo alternativos, como esclarece o Grupo de Trabalho do Artigo 29.º (doravante, "GT29") nas Orientações relativas à transparência na aceção do Regulamento 2016/679. Cfr. "Orientações relativas à transparência na aceção do Regulamento 2016/679", GT29, acesso em 2 de abril de 2020, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227. Sendo certo que as Orientações do GT29 (atualmente o Comité Europeu de Proteção de Dados) não são vinculativas, estas representam a opinião partilhada das várias Autoridades de Controlo dentro da União Europeia. Para uma análise mais detalhada sobre esta questão *vd.* Rita de Sousa Costa, *A realização do direito da protecção de dados da União Europeia através das fontes não-legislativas: dos grandes temas jurisprudenciais aos desafios do soft law, no contexto da aplicação do Regulamento Geral sobre a Protecção de Dados* (Dissertação de Mestrado: Universidade Católica Portuguesa, 2019).
[3] Uma exigência que também é vigente para informação e comunicações ao abrigo do artigo 15.º a 22.º e 34.º do RGPD (artigo 12.º, n.º 1 e Considerando 39 do RGPD).
[4] A verdade é que não se consegue antever nenhuma situação em que a exceção à gratuitidade presente no artigo 12.º, n.º 5, se possa manifestar no contexto do simples Direito à Informação dos artigos 13.º e 14.º do RGPD. Esta exceção poderá manifestar-se se estivermos perante pedidos manifestamente infundados ou excessivos, designadamente se revestirem um caráter repetitivo nos artigos 15.º a 22.º e 34.º. Isto inclui, naturalmente, a informação a ser prestada no âmbito do Direito de Acesso (artigo 15.º). Cabe ao responsável pelo tratamento demonstrar que os requisitos para a aplicação desta norma se encontram preenchidos.

diferencie adequadamente da restante informação prestada ao titular dos dados. Informação que seja de difícil compreensão, confusa ou avassaladora pode corresponder a uma violação das disposições de proteção de dados.

Neste sentido, o responsável pelo tratamento deverá, por exemplo, evitar informações e regras relativas à proteção de dados enxertadas nos Termos e Condições de um *website* ou aplicação. Igualmente é desaconselhado que tente integrar, na mesma cláusula contratual, disposições sobre privacidade aglomeradas no tratamento de outras matérias. Certamente será preciso conduzir um juízo de ponderação, na medida em que, em matérias conexas à proteção de dados (como seja a cibersegurança), poderá haver boas razões (e inclusive benefícios para o titular dos dados) para apresentar informação aprofundada no mesmo local.

Adicionalmente, importa referir que o facto de a Comissão não ter ainda adotado ícones normalizados no âmbito do artigo 12.º, n.os 7 e 8 não deve ser visto como impeditivo à utilização de ícones, imagens e outro tipo de auxiliares visuais pelos responsáveis pelo tratamento como meio complementar de prestação de informação – caso se considere que tal utilização trará benefícios quanto à clareza dos elementos facultados ao titular dos dados[5].

O RGPD estipula critérios ligeiramente distintos relativamente à informação que seja recolhida diretamente junto dos titulares dos dados ou indiretamente. Quando a recolha seja direta, nos termos do artigo 13.º do RGPD, o responsável pelo tratamento deverá providenciar a seguinte informação:

a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
b) Os contactos do encarregado da proteção de dados, se for caso disso;
c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico[6] para o tratamento;
d) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f) do RGPD, os interesses legítimos do responsável pelo tratamento ou de um terceiro;
e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
f) Informação relativa a transferências de dados para países terceiros, nos termos do artigo 13.º, n.º 1, al. f);
g) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
h) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;
i) Quando o fundamento de licitude aplicável for o consentimento do titular dos dados, o direito à retirada do consentimento;
j) O direito de apresentar reclamação a uma autoridade de controlo;

[5] A utilização de símbolos e pictogramas como auxiliar informativo oferece vantagens que não devem ser desconsideradas no âmbito da proteção de dados pessoais, pois o seu titular terá maior propensão para identificar um símbolo do que para ler vários parágrafos por vezes complexos. Sobre o tema, cfr. A. Barreto Menezes Cordeiro, *Direito da Proteção de Dados. À luz do RGPD e da Lei n.º 58/2019* (Coimbra: Almedina, 2020), 389 e Colette R. Brunschwig, *"Humanoid robots for contract visualisation"*, UNIO - EU Law Journal, 6, 1 (2020): 142-160.

[6] Referindo-se aqui ao fundamento de licitude do artigo 6.º, ou dos artigos 6.º e 9.º quando haja tratamento de categorias especiais de dados.

k) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados; e

l) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.os 1 e 4 do RGPD, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados[7].

Existe uma exceção ao dever de prestar informação no âmbito do artigo 13.º do RGPD: o conhecimento prévio por parte do titular dos dados das informações que seriam legalmente exigíveis[8]. No entanto, neste caso, chama-se a atenção para a necessidade de o responsável pelo tratamento documentar a não prestação da informação e os motivos que levaram a esta escolha. Esta documentação será particularmente pertinente quando as autoridades de controlo e/ou os Tribunais sejam chamados a avaliar a opção pela não prestação de informação, nos termos anteriormente elencados.

O leque de informações a prestar ao titular dos dados no âmbito do artigo 14.º diverge apenas de forma ligeira em relação ao artigo 13.º. Não existe, no artigo 14.º, norma equivalente à do artigo 13.º, n.º 2, al. e). No entanto, para acautelar a situação da recolha indireta dos dados, neste caso, para além do supracitado, passa a ser necessário informar o titular também sobre:

a) As categorias dos dados pessoais em questão; e

b) A origem dos dados pessoais e, eventualmente, se provêm de uma fonte acessível ao público.

[7] Sobre o âmbito de aplicação deste artigo cfr. Tiago Sérgio Cabral, *AI Regulation in the European Union…*, 150 e ss.; Tiago Sérgio Cabral, "O "Juiz artificial": breves notas sobre a utilização de inteligência artificial pelos Tribunais e a sua relação com a legislação europeia de proteção de dados", in *O Contencioso da União Europeia e a cobrança transfronteiriça de créditos: compreendendo as soluções digitais à luz do paradigma da Justiça eletrónica europeia (e-Justice)*, Joana Covelo de Abreu, Larissa Coelho e Tiago Sérgio Cabral coord. (Braga: Escola de Direito da Universidade do Minho, 2020), 115-141; Gianclaudio Malgieri, *"Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards"in the national legislation"*, Computer Law & Security Review (2019): 1-26; "European Union regulations on algorithmic decision-making and a "right to explanation"", Bryce Goodman and Seth Flaxman, accessed August 17, 2019, https://arxiv.org/abs/1606.08813; Sandra Wachter, Brent Mittelstadt and Chris Russell, *"Counterfactual Explanations Without Opening the Black Box: Automated Decisions And The GDPR"* Harvard Journal of Law & Technology 31,2 (2018): 841-887; Mireille Hildebrandt, *"Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning"* 20,1 (2019): 83-122; "The Right to Explanation, Explained", Margot E. Kaminski, https://osf.io/preprints/lawarxiv/rgeus/download; Gianclaudio Malgieri, *"Trade Secrets v Personal Data: a possible solution for balancing rights"*, International Data Privacy Law 6,2 (2016): 102-116; Iakovina M. Kindyldi, *Smart Companies: Company & Board Members Liability in the Age of AI* (Dissertação de Mestrado: Tilburg University, 2018); Iakovina M. Kindyldi, *"Smart Companies: Company & Board Members Liability in the Age of AI"*, UNIO - EU Law Journal. 6,1 (2020): 115-141. "Is there a right to explanation' for machine learning in the GDPR?", Andrew Burt, accessed June 17, 2019, "Artificial Intelligence and Privacy", Datatilsynet, acesso em 15 de fevereiro, 2020; https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf; Sandra Wachter, Brent Mittelstadt and Luciano Floridi, *"Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation"*, International Data Privacy Law 7, 2 (2017): 79-99; AEPD. 'Adecuación al RGPD de Tratamientos Que Incorporan Inteligencia Artificial. Una Introducción'. Accessed 25 February 2020. https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf.

[8] Quando o responsável pelo tratamento tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, o responsável terá de fornecer, antes desse tratamento, ao titular dos dados, informações sobre esse fim e quaisquer outras informações pertinentes, de acordo com o artigo 13.º, n.º 3 do RGPD. No artigo 14.º, a norma equivalente encontra-se no n.º 4.

Estas duas adições prendem-se com a necessidade de informar o titular dos dados sobre aspetos que poderá desconhecer, tendo em conta que a recolha não ocorreu junto do titular. Naturalmente, quando a recolha seja direta, o titular saberá tanto as categorias dos dados recolhidos, porque as está a facultar, como a sua origem, sendo o próprio titular que coloca os dados ao dispor do responsável pelo tratamento.

As exceções que permitem a não prestação de informação são igualmente mais amplas neste artigo incluindo, para além do conhecimento prévio, situações em que exista impossibilidade ou esforço desproporcionado (artigo 14.º, n.º 5, al. b do RGPD), previsão expressa em legislação (artigo 14.º, n.º 5, al. c do RGPD) e obrigação de sigilo profissional que obste à prestação da informação (artigo 14.º, n.º 5, al. d do RGPD). Como acima aventado, o responsável do tratamento continua sempre adstrito à documentação da opção de não prestação de informação[9].

2.2. Direito de Acesso

O artigo 15.º do RGPD concede aos titulares dos dados o direito a obter confirmação de que os dados que lhes dizem respeito estão a ser objeto de tratamento, a ter acesso a estes mesmos dados em caso afirmativo, bem como a obter cópia dos dados pessoais em fase de tratamento[10].

[9] Cfr. Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Cham: Springer: 2018); 141 e ss.; Peter Carey, *Data Protection: A Practical Guide to UK and EU Law* (5:ª ed, Oxford: Oxford University Press, 2018), 123 e ss; "Guide to the General Data Protection Regulation", Information Commissioner's Office, acesso em 20 de abril de 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/; Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, *The Standard Data Protection Model A method for Data Protection advising and controlling on the basis of uniform protection goals* (v. 2b, Mecklenburg-Vorpommern: AK Technik of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, 2020), 27 e ss.

[10] Caso o titular dos dados solicite cópias adicionais, o responsável poderá cobrar, pelo tratamento, uma taxa razoável tendo em conta os custos administrativos para o seu fornecimento (artigo 15.º, n.º 3 do RGPD). Cabe, no entanto, promover a sua leitura em conjugação com o artigo 12.º, n.º 5 do RGPD: neste artigo expressamente se determina que será aplicável a "quaisquer comunicações e medidas tomadas nos termos dos artigos 15.º a 22.º", pelo que, "[s]e os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, o responsável pelo tratamento pode" exigir o pagamento de taxa razoável atentos os custos administrativos suportados (artigo 12.º, n.º 5, al. a do RGPD) ou recusar o seguimento do pedido (artigo 12.º, n.º 5, al. b do RGPD). Assim, se a compatibilização de ambos os regimes introduz alguma clareza quanto aos pedidos repetitivos/de fornecimento de novas cópias – podendo-lhes o responsável pelo tratamento associar uma taxa administrativa –, parece nebulosa nos casos de recusa, pelo responsável pelo tratamento, ao exercício do direito de acesso. Deste modo, no primeiro caso, poderão cobrar-se taxas associadas ao esforço administrativo no caso da reiteração desproporcionada de pedidos de acesso (tal parece ser o espírito da leitura combinada dos artigos 15.º, n.º 3 e 12.º, n.º 5 do RGPD). Já quanto aos casos de recusa, apesar de expressa e literalmente consagrada no artigo 12.º, n.º 5, al. b do RGPD, foi afastada da literalidade do artigo 15.º. Tal compatibilização da interpretação das normas em causa mereceria uma atenção particular, nomeadamente através de um reenvio prejudicial de interpretação, à luz do artigo 267.º do Tratado sobre o Funcionamento da União Europeia. Ainda assim, chamamos a atenção para o facto de um pedido do titular dos dados dificilmente poder ser considerado como infundado ou excessivo caso tenha havido uma alteração ou adição relevante aos dados recolhidos sobre si pelo responsável pelo tratamento, desde o momento do seu último pedido. A implementação de um sistema eletrónico seguro para acesso aos dados poderá ser uma solução adequada para os responsáveis pelo tratamento que recolham dados em permanência.

Neste ponto, importa salientar que o conceito de tratamento de dados ao abrigo do RGPD é bastante amplo. Desta forma, a simples conservação (*storage*) de dados pessoais, sem nenhum outro tipo de tratamento, será o suficiente para que o responsável pelo tratamento esteja obrigado ao cumprimento das normas do direito de acesso. O conceito é tão amplo que dispensa a discussão relativa aos tratamentos atuais *versus* tratamentos transcorridos. Caso o responsável pelo tratamento tenha alguma informação sobre o titular dos dados que se deva considerar como dado pessoal, incluindo potencial documentação referente a tratamentos antigos cuja maioria dos dados já tenha sido apagada, deve facultar a confirmação do tratamento e a informação legalmente requerida ao titular dos dados.

Por outro lado, a faculdade que parece ser reconhecida pelo Comité Europeu de Proteção de Dados (que substituiu o GT29 ao abrigo do RGPD) de os responsáveis pelo tratamento conservarem dados enquanto forem necessários para a sua defesa em processo judicial – ainda que o tratamento tenha de ser restrito apenas a esta finalidade e devam ser implementadas medidas técnicas e organizativas para assegurar que os dados não podem ser acedidos para outras finalidades –, salvaguarda que a informação estará lá, também para os titulares de dados, a fim de que possam acionar os responsáveis pelo tratamento por eventuais violações do RGPD que incidam sobre os seus dados[11].

Adicionalmente, quando o titular dos dados exerça o seu Direito de Acesso deve ainda ser-lhe fornecido um conjunto de informações relevantes, nomeadamente:

a) As finalidades do tratamento dos dados;
b) As categorias dos dados pessoais em questão;
c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;
d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;
e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;
f) O direito de apresentar reclamação a uma autoridade de controlo;
g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;
h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.^{os} 1 e 4 do RGPD, e, pelo menos nesses casos,

[11] Cfr. "Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications [version for public consultation]", Comité Europeu de Proteção de Dados, acesso em 19 de abril de 2020, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en. Levantando a questão dos tratamentos atuais contra os tratamentos transcorridos *vd.* A. Barreto Menezes Cordeiro, *Direito da Proteção de Dados…,* 263; "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", GT29, acesso em 5 de abril, 2020; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053; Magda Cocco e Joana Neves, "Ubi jus, ubi remedium – reflexões acerca do direito à ação judicial e do direito de indemnização contra o responsável pelo tratamento ou o subcontratante", in *O Contencioso da União Europeia e a cobrança transfronteiriça de créditos: compreendendo as soluções digitais à luz do paradigma da Justiça eletrónica europeia (e-Justice)*, Joana Covelo de Abreu, Larissa Coelho e Tiago Sérgio Cabral coord. (Braga: Escola de Direito da Universidade do Minho, 2020), 96-113.

> informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados[12].

Fica a questão de saber se as informações que são facultadas ao titular dos dados ao abrigo do Direito de Acesso devem ser as mesmas que lhe foram facultadas ao abrigo do Direito à Informação nos termos dos artigos 13.º e 14.º do RGPD[13]. Infelizmente, o âmbito deste texto não nos permite discorrer de forma profunda sobre esta questão[14]. Na realidade, as Orientações do GT29 sobre as decisões individuais automatizadas sublinham que a informação a ser prestada nos termos do artigo 15.º já deveria ter sido facultada ao titular dos dados em linha com as obrigações do Direito à Informação propriamente ditas (artigos 13.º e 14.º)[15]. Com este esclarecimento, o GT29 tentou recordar, aos responsáveis pelo tratamento, a necessidade de conduzir o tratamento de dados nos termos indicados ao seu titular no momento da prestação de informações, demandando-se uma correspondência entre o conteúdo e o objeto da prestação de informações e o conteúdo e o objeto do tratamento realizado. Tal não obsta a que o responsável, tendo exponenciado o tratamento, cumpra escrupulosamente o direito de acesso, na medida em que este pressupõe que o responsável pelo tratamento preste sempre a informação mais atualizada que esteja ao seu dispor. Por natureza, poderá existir informação mais desenvolvida ou atualizada no contexto do Direito de Acesso, pois é fornecida num período temporal subsequente.

Um exemplo particularmente interessante será o das decisões individuais automatizadas – especialmente quanto tomadas por algoritmos de inteligência artificial na sua vertente de *machine learning* – onde uma interpretação restritiva poderá inviabilizar a prestação de informação sobre a decisão específica. Quando presta informação nos termos do artigo 13.º, dificilmente o responsável pelo tratamento estará em condições para fazer mais do que prestar informação sobre o funcionamento do sistema, uma vez que os dados ainda não foram efetivamente tratados e não existe uma decisão específica. Só após a prestação de informação e subsequente tratamento lícito de dados, poderá ser aplicado o modelo matemático a um conjunto específico de dados, dando origem a uma decisão sobre aquele titular dos dados. Idealmente, nesse momento, o responsável pelo tratamento estará em condições para prestar informação sobre os aspetos mais importantes que foram tidos em conta na tomada de decisão (dentro dos milhões que a máquina pode ter aprendido e utilizado). No fim de todo este processo, caso o titular dos dados exerça o seu Direito de Acesso, não há qualquer razão – e de facto, seria mesmo contra a lógica do RGPD – para não prestar esta informação que aparece subsequentemente, mas que poderá ser relevante para perceber se existe potencial discriminação algorítmica ou outro tratamento ilícito de dados[16].

---

[12] Quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas, nos termos do artigo 46.º relativo à transferência de dados (artigo 15.º, n.º 2.º do RGPD).

[13] Lembramos que, mesmo que a redação dos artigos seja bastante semelhante a nível de informação, não é absolutamente idêntica.

[14] Já tivemos oportunidade de o fazer noutras sedes, para as quais remetemos para uma análise mais profunda desta questão. Cfr. Tiago Sérgio Cabral, *AI Regulation in the European Union: …,* 175 e ss.

[15] "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", WP29, acesso em 5 de abril, 2020, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826

[16] Tiago Sérgio Cabral, *AI Regulation in the European Union: …,* 175 e ss; Alexandre Veronese, Alessandra Silveira e Amanda Nunes Lopes Espiñeira Lemos, *"Artificial intelligence, Digital Single Market and the proposal of a right to fair and reasonable inferences: a legal issue between ethics and techniques",* UNIO EU Law Journal 5, 2 (2019): 75-91.

No âmbito da obrigação que recai sob o responsável pelo tratamento de facilitar o exercício dos direitos pelo titular dos dados, *"deverão ser previstas regras para facilitar o exercício pelo titular dos dados dos direitos que lhe são conferidos ao abrigo do presente regulamento, incluindo procedimentos para solicitar e, sendo caso disso, obter a título gratuito, em especial, o acesso a dados pessoais, a sua retificação ou o seu apagamento e o exercício do direito de oposição. O responsável pelo tratamento deverá fornecer os meios necessários para que os pedidos possam ser apresentados por via eletrónica, em especial quando os dados sejam também tratados por essa via"* (Considerando 59). Em especial, no caso do Direito de Acesso, quando tal seja viável, o responsável pelo tratamento deverá colocar ao dispor do titular dos dados um sistema eletrónico seguro, que possibilite o acesso direto aos seus dados pessoais (Considerando 63). Parece em tudo lógico que o mesmo sistema deva ser capaz de fornecer cópia dos dados pessoais em fase de tratamento em formato eletrónico de uso corrente, nos termos do artigo 15.º, n.º 3. Idealmente, e se os pressupostos deste estiverem preenchidos, deve permitir também que os titulares dos dados exportem os seus dados em formato estruturado, de uso corrente e de leitura automática, assegurando a conformidade do tratamento também com o Direito à Portabilidade.

Segundo o Considerando 63[17], o Direito de Acesso e a prestação de informações ao titular dos dados não deve "*prejudicar os direitos ou as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o software".* A questão a deslindar é se estaremos aqui perante uma restrição aos direitos dos titulares dos dados, como tem sido defendido por alguns autores[18]. Primeiramente, uma restrição desta índole dificilmente poderia ser estabelecida por um Considerando, dada a sua eficácia meramente interpretativa e a falta de reflexo de uma regra deste tipo no articulado do RGPD (certamente não se encontra expressamente no artigo 15.º, n.º 4 do RGPD). Em segundo lugar, da leitura atenta do próprio Considerando decorre que, de facto, este até onera de

[17] Nos termos do artigo 296.º do TFUE, quando provenientes de fonte da UE, *"os atos jurídicos são fundamentados e fazem referência às propostas, iniciativas, recomendações, pedidos ou pareceres previstos pelos Tratados"*. Nestes termos a existência de Considerandos é um requisito legal cuja omissão comina na invalidade do ato. Este requisito é aplicável a todos os atos que tenham como objetivo produzir efeitos jurídicos na esfera de terceiros. Ainda que resulte claro da jurisprudência do Tribunal de Justiça da União Europeia ("TJUE") que os Considerandos não são vinculativos e que de nenhuma maneira podem ser utilizados para procurar a derrogação das disposições operativas quando a estas sejam contrários, como bem explicado pelo TJUE em *Casa Fleischhandels,* o Considerando *"pode permitir esclarecer a interpretação a dar a uma regra de direito"*. Já em *Giuseppe Manfredi* o TJUE afirma que o Considerando *"não pode ser invocado para interpretar [o ato] num sentido manifestamente contrário à sua redacção"*. Assim, neste contexto, poderá entender-se que o TJUE vislumbra os Considerandos como úteis à interpretação do ato em todas as ocasiões em que não são manifestamente contrários à sua redação. Salvo devidamente assinalado, no contexto do presente texto, nenhum dos Considerandos aqui analisados é manifestamente contrário à redação das normas a que se referem no regime de proteção de dados. Na verdade, estão em perfeita sintonia com aquela que é a lógica subjacente aos instrumentos normativos, devendo assim ser adequadamente considerados no esforço de interpretação da norma. Cfr. "Complexity of EU law in the domestic implementing process", Roberto Baratta, acesso em 2 de março, 2020, http://ec.europa.eu/dgs/legal_service/seminars/20140703_baratta_speech.pdf; Roberto Baratta, *"Complexity of EU Law in the Domestic Implementing Process",* The Theory and Practice of Legislation 2, 3 (2014): 293-308, Gianclaudio Malgieri and Giovanni Comande, *"Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation",* International Data Privacy Law 7, 4 (2017): 243-265; Tiago Sérgio Cabral, *"A short guide to the legislative procedure in the European Union"*, UNIO - EU Law Journal, 6, 1 (2020): 161-180.; Acórdão do TJUE de 25 de novembro de 1998, *Giuseppe Manfredi v. Regione Puglia*, Processo C–308/97, ECLI:EU:C:1998:566; Acórdão do TJUE de 13 de julho de 1989, *Casa Fleischhandels v. Bundesanstalt für landwirtschaftliche Marktordnung*, Processo 215/88, ECLI:EU:C:1989:331.

[18] Em especial, Sandra Wachter, Brent Mittelstadt and Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" …, 79-99.

forma pesada o responsável pelo tratamento, procurando obrigá-lo a encontrar uma forma de fornecer a informação e acesso legalmente prescritos ao titular dos dados sem colocar em causa outros bens jurídicos de relevo. Claro está que, por exemplo, o responsável pelo tratamento nunca teria de fornecer acesso ao código-fonte ou a todos os fatores que fossem tidos em conta numa decisão individual automatizada, mas teria de fornecer, pelo menos, indicações relevantes sobre os fatores mais importantes e sobre o funcionamento do sistema que levou a esta decisão. Nestes termos se, por alguma razão, o responsável pelo tratamento estiver em condições de fornecer ao titular dos dados informação com um maior nível de especificidade no âmbito do Direito de Acesso, em relação àquela que ofereceu no âmbito do Direito à Informação deve, em cumprimento dos princípios gerais do RGPD, fazê-lo[19].

2.3. Direito à Retificação

O Direito à Retificação deve ser considerado como um corolário natural do princípio da exatidão. O tratamento de dados inexatos não favorece, em princípio, nem o responsável pelo tratamento nem o titular dos dados. Adicionalmente, o titular dos dados poderá encontrar-se numa posição mais favorável, quando comparado com o responsável pelo tratamento, para fornecer dados com um maior nível de fiabilidade e exatidão e, como tal, de maior utilidade no contexto de operações de tratamento de dados.

Desta forma, o artigo 16.º do RGPD comporta duas dimensões. Por um lado, é conferido ao titular dos dados o direito de obter a retificação, sem demora injustificada, dos dados pessoais que lhe digam respeito. Por outro lado, o titular tem também o direito a ver completados dados pessoais seus que estejam a ser tratados e não se encontrem completos (mesmo que, em bom rigor, os existentes não sejam inexatos).

Relativamente à retificação propriamente dita, importa atentar na dualidade entre dados objetivos e dados subjetivos[20]. Os dados objetivos permitem que, do confronto entre a informação que está na posse do responsável pelo tratamento com a nova informação facultada pelo titular dos dados, se possa concluir, sem espaço para ambiguidade, pela discrepância/desconformidade da primeira com a realidade. Por seu turno, os dados subjetivos são aqueles cuja impossibilidade de aferir a exatidão resulta da sua própria natureza, aqui incluídos determinados gostos/preferências, opiniões e juízos de valor.

Os dados objetivos poderão ser retificados quando se encontrem preenchidos os requisitos constantes do artigo 16.º do RGPD. A confirmação da exatidão dos novos dados, mesmo que objetivos, mediante os quais se pretende retificar os antigos, poderá onerar de forma relevante o titular dos dados. Um exemplo relacionado com tecnologias recentes, será o de dados pessoais que sejam extraídos através do processamento de *big data*. Na verdade, estes continuam a ser dados pessoais que derivam do tratamento de outros dados pessoais (em grande quantidade). Caso o titular dos dados altere, através da retificação, um dos

[19] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation …*; 150 e ss.; Peter Carey, *Data Protection…*, 126 e ss; "Guide to the General Data Protection Regulation", Information Commissioner's Office, acesso em 20 de abril de 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.
[20] Cfr. A. Barreto Menezes Cordeiro, *Direito da Proteção de Dados…,* 270-272.

pressupostos nos quais se baseia a conclusão final, poderá ser necessário repetir todas as operações de tratamento adicionais para percecionar se esta conclusão se mantém.

Os mecanismos associados ao direito em apreço não serão, propriamente, os mais adequados para retificar dados subjetivos. Ainda assim, os pressupostos objetivos que estejam na base de um dado subjetivo podem ser questionáveis por esta via. Outros direitos poderão ser mais adequados para endereçar a matéria dos dados subjetivos. De qualquer forma, um dado subjetivo face ao qual não exista fundamento de licitude adequado para o seu tratamento está sujeito ao Direito ao Apagamento.

Relativamente a dados que não estejam completos e sejam objeto de tratamento, já não se está perante uma questão de exatidão propriamente dita, mas sim perante uma questão de suficiência/completude. O titular dos dados tem, no fundo, o direito a não ser afetado por operações de tratamento nas quais não se avalie a sua situação de forma adequada.

Este direito só terá relevo no caso de os dados incompletos serem relevantes no âmbito da finalidade subjacente ao tratamento de dados. Por exemplo, se determinado responsável pelo tratamento tiver solicitado o endereço de *email* ao titular dos dados para o envio de uma *newsletter*, e estando este endereço de *email* correto, não deverá o titular solicitar que os seus dados venham a ser completados (com o seu nome completo e morada), se esta informação não revestir relevância no contexto do tratamento. Caso o titular dos dados o solicite, o responsável pelo tratamento deverá recusar, sob pena de estarmos perante uma violação do princípio da minimização[21].

2.4. Direito ao Apagamento

Este foi, talvez, pelo menos numa primeira fase, o mais mediático dos direitos conferidos aos titulares dos dados pelo RGPD. Nos termos do artigo 17.º do RGPD, o titular dos dados pode obter, do responsável pelo tratamento, o apagamento dos seus dados pessoais quando determinados requisitos legais se encontrarem cumpridos. O apagamento dos dados deve acontecer "*sem demora injustificada*" – o que nos remete para a problemática de definir o que se entende por demora justificada num contexto tecnológico como aquele em que muitas vezes se aplica o RGPD. Nos termos do artigo 12.º do RGPD, o responsável pelo tratamento deve fornecer ao titular dos dados informações sobre as medidas tomadas no seguimento dos pedidos apresentados pelo último – e de acordo com os artigos 15.º a 20.º, no prazo de um mês a contar da receção do pedido. Este prazo poderá ser prorrogado por até mais dois meses, caso o pedido seja especialmente complexo e/ou quando o número de pedidos assim o justifique[22].

[21] Neste sentido, A. Barreto Menezes Cordeiro, *Direito da Proteção de Dados…*, 272 e 273.

[22] A versão portuguesa do RGPD enferma, neste artigo, de uma tradução que, não estando incorreta, não resulta propriamente feliz. Enquanto a versão inglesa – língua de negociação do RGPD – prevê de forma bastante clara que *"that period may be extended by two further months where necessary, taking into account the complexity and number of the requests"*, não deixando dúvidas quanto à soma total de três meses, a versão portuguesa dispõe que *"esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos"*, deixando sérias dúvidas sobre se se trata de um prazo total de dois ou três meses. Ademais, as versões espanhola, francesa e italiana parecem estar em concordância com a versão inglesa. Posto isto, é de referir que o Conselho lançou uma errata para tentar corrigir os equívocos nas traduções do RGPD. No entanto,

No entanto, de acordo com artigo 17.º do RGPD, o conceito de "sem demora injustificada" não será necessariamente coincidente com o prazo limite para fornecer, ao titular dos dados, informação sobre as medidas tomadas no seguimento dos pedidos apresentados.

Em casos específicos, como seja o da inteligência artificial, e especialmente em termos de *datasets* utilizados por algoritmos de *machine learning*, quando *i)* o apagamento possa causar sérias dificuldades ao funcionamento contínuo do algoritmo, *ii)* o grau de responsabilidade do responsável pelo tratamento seja diminuto em relação ao motivo do apagamento (por exemplo, existiu apenas uma retirada de consentimento e não se trata de um caso de tratamento ilícito de dados) e/ou *iii)* o apagamento possa causar dano a outros utilizadores da ferramenta tecnológica, deve considerar-se que podem existir situações de demora justificada superior a três meses.

Quando assim seja, o responsável pelo tratamento deve, nos termos do artigo 12.º do RGPD, informar o titular dos dados do início das diligências para executar o seu Direito ao Apagamento, das razões que levam ao atraso e manter o titular dos dados informado de qualquer desenvolvimento que surja.

Esta situação poderá revelar-se quando um determinado *dataset* for dotado de um número de entradas diminuto relativo, por exemplo, a uma determinada minoria étnica. Neste caso, a retirada de um número relevante de entradas de indivíduos pertencentes a esta minoria poderá desembocar numa situação de discriminação algorítmica relativamente a todas as pessoas a que a ela pertençam. Cabe tanto aos responsáveis pelo tratamento, como às autoridades de controlo e, mesmo ao julgador, fazer o adequado teste de proporcionalidade entre os interesses individuais e o interesse público em evitar, ao máximo, o problema da discriminação algorítmica com todas as consequências negativas que acarreta.

Com a devida atenção a estas considerações, em princípio, o titular dos dados terá Direito ao Apagamento nos seguintes casos:

a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;
c) O titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2;
d) Os dados pessoais foram tratados ilicitamente;
e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;

para além de questões sobre a validade jurídica do instrumento, a errata não foi capaz de suprir todas as questões relativas à tradução do diploma, restando este descompasso aparente entre a versão portuguesa e as demais versões mencionadas.

f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1.

No entanto, nos termos e com as limitações prescritas no artigo 17.º, n.º 3 do RGPD, o responsável pelo tratamento poderá recusar o apagamento quando o tratamento de dados se revele necessário:

i) Ao exercício da liberdade de expressão e de informação;
ii) Ao cumprimento de uma obrigação legal que exija o tratamento, exercício de funções de interesse público, ou ao exercício da autoridade pública quando a tal esteja adstrito o responsável pelo tratamento;
iii) Por motivos de interesse público no domínio da saúde pública;
iv) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos; ou ainda
v) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Não devemos olvidar as responsabilidades de comunicação do exercício dos direitos que podem recair sob o responsável pelo tratamento de acordo com o artigo 17.º, n.º 2 do RGPD e do Considerando 66[23]. Ademais, nos termos do artigo 19.º do RGPD, o responsável pelo tratamento deverá igualmente *"comunicar a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a que se tenha procedido (…) salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado. [Adicionalmente, s]e o titular dos dados o solicitar, o responsável pelo tratamento fornece-lhe informações sobre os referidos destinatários"*[24].

[23] Nos termos do artigo 17.º, n.º 2 do RGPD, "*quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los [nos termos do artigo 17.º, n.º 1], toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos*". O Considerando 66 acompanha esta norma ao afirmar que "*para reforçar o direito a ser esquecido no ambiente por via eletrónica, o âmbito do direito ao apagamento deverá ser alargado através da imposição ao responsável pelo tratamento que tenha tornado públicos os dados pessoais da adoção de medidas razoáveis, incluindo a aplicação de medidas técnicas, para informar os responsáveis que estejam a tratar esses dados pessoais de que os titulares dos dados solicitaram a supressão de quaisquer ligações para esses dados pessoais ou de cópias ou reproduções dos mesmos. Ao fazê-lo, esse responsável pelo tratamento deverá adotar as medidas que se afigurarem razoáveis, tendo em conta a tecnologia disponível e os meios ao seu dispor, incluindo medidas técnicas, para informar do pedido do titular dos dados pessoais os responsáveis que estejam a tratar os dados*".

[24] Acordão do TJUE de 13 de maio de 2014, *Google Spain v. Agencia Española de Protección de Datos*, Processo C-131/12, ECLI:EU:C:2014:317; Acórdão do TJUE de 24 de setembro de 2019, *Google v. CNIL*, Processo C-507/17, ECLI:EU:C:2019:772; "Google v. CNIL: Is a new landmark judgment for personal data protection on the horizon?", Alessandra Silveira e Tiago Sérgio Cabral, acesso em 2 de abril de 2020, https://officialblogofunio.com/2019/09/10/editorial-of-september-2019/; Eduard Fosch Villaronga, Peter Kieseberg e Tiffany Li, "*Humans Forget, Machines Remember: Artificial Intelligence and The Right to Be Forgotten*" Computer Law & Security Review 32,2 (2018):304-313; Nadezhda Purtova, *"The law of everything. Broad concept of personal data and future of EU data protection law"* Law, Innovation and Technology 10,1 (2018): 40-81; "Guía de Privacidad desde el Diseño", AEPD, acesso em 2 de abril de 2020, https://www.aepd.es/media/guias/guia-privacidad-desde-diseno.pdf; Viktor Mayer-Schönberger, *delete: The Virtue of Forgetting in the Digital Age* (New Jersey: Princeton University Press, 2009): 37-58.

2.5. Direito à Limitação do Tratamento

O Direito à Limitação do Tratamento tem natureza de um direito provisório – ou seja, está restrito no tempo e persiste enquanto a condição que deu origem à limitação não desaparecer – sendo, em princípio, substituído pelo exercício de um direito com características de maior perenidade. O titular dos dados pode exercer tal direito perante o responsável pelo tratamento nas seguintes circunstâncias:

a) No âmbito do Direito à Retificação, quando contestar a exatidão dos dados pessoais, e no período no qual o responsável pelo tratamento procede à análise destinada a saber da necessidade efetiva de retificação;
b) Quando o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;
c) Quando o tratamento dos dados pessoais já não for necessário para os fins que motivaram a sua recolha, mas sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;
d) Quando o titular exercer o seu Direito de Oposição, até que se verifique a existência ou ausência de razões imperiosas e legítimas do responsável pelo tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados.

De acordo com o artigo 4.º, n.º 3.º, do RGPD, limitação ao tratamento está definida como *"a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro"*. Aqui se pode encontrar mais um exemplo de tradução porventura equivocada da versão portuguesa do RGPD que pode levar o intérprete a ser induzido em erro e a considerar que a limitação do tratamento é um conceito mais restrito do que aquele que, na verdade, se pretende com o diploma. Nisto, para clarificação, chama-se a atenção para a definição da versão inglesa do RGPD (língua na qual o normativo foi negociado): *"restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future"*[25]. Deste modo, a versão portuguesa deveria considerar que a limitação do tratamento consiste na "marcação dos dados pessoais". O Considerando 67 oferece, de seguida, um importante auxiliar interpretativo sobre como poderão ser marcados os dados pessoais. Segundo este Considerando: *"pode recorrer-se a métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio web dos dados aí publicados. Nos ficheiros automatizados, as [limitações] ao tratamento deverão, em princípio, ser impostas por meios técnicos de modo a que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados. Deverá indicar-se de forma bem clara no sistema que o tratamento dos dados pessoais se encontra sujeito a limitações"*[26]. Refira-se que a tradução equivocada poderá mesmo levar o intérprete a considerar que o Considerando 67 é incompatível com o articulado do RGPD, algo que não corresponde à realidade.

[25] Na mesma linha vão, por exemplo, as versões francesa e espanhola do RGPD.
[26] Outro equívoco de tradução existe neste Considerando, uma vez que a versão portuguesa do RGPD traduz, aqui, *restrictions* como "restrições" ao passo que, nas disposições sobre o Direito à Limitação do Tratamento, traduz *restriction* como "limitação". Erroneamente poderá pensar-se que estamos perante conceitos diferentes, mas não é este o caso.

Quando o tratamento dos dados esteja limitado, o responsável pelo tratamento não deverá encetar nenhuma operação de tratamento diferente da conservação dos próprios dados. Neste conceito, deve considerar-se que estão incluídas também operações acessórias quando estas sejam estritamente necessárias para salvaguardar a correta conservação dos dados. Por exemplo, em caso de falha iminente do suporte de conservação dos dados limitados, poderá o responsável pelo tratamento proceder a uma operação de cópia dos dados pessoais para garantir que não são perdidos. Adicionalmente, estes dados poderão ser tratados para outros fins quando exista consentimento do titular dos dados, motivos ponderosos de interesse público da União ou de um Estado-Membro, para efeitos de declaração, exercício ou defesa de um direito num processo judicial ou na defesa dos direitos de outra pessoa singular ou coletiva[27].

2.6. Direito de Portabilidade

Como tivemos oportunidade de explicar anteriormente, o RGPD não tem apenas como objetivo salvaguardar a proteção dos dados pessoais dos seus titulares. Em igualdade de circunstâncias está a salvaguarda do mercado único, mormente o mercado único digital, absolutamente essencial para o crescimento da União Europeia, bem como a relevância que, neste contexto, pode ter a livre circulação dos dados pessoais, desde que observadas as demandas de proteção efetiva do titular.

Em abstrato, é possível que um *player* de mercado, onde o titular tenha depositado os seus dados, possa encetar um *lock-in* daqueles dados ao seu serviço ou plataforma. De forma idêntica, a dificuldade em "transportar" os dados de um serviço ou plataforma para a outra poderá afetar a livre concorrência no mercado e, por conseguinte, a posição do consumidor europeu.

Posto isto, o Direito à Portabilidade de dados existirá quando o fundamento de licitude for o consentimento do titular dos dados ou a execução de um contrato no qual o titular dos dados é parte ou para diligências pré-contratuais a pedido do titular dos dados. Este direito incide apenas sobre os dados que digam respeito ao titular dos dados e que este tenha fornecido ao responsável pelo tratamento. De acordo com o GT29[28], este conceito engloba o fornecimento ativo e passivo de dados pelo titular dos dados. Isto é, encontram-se dentro do âmbito de aplicação do Direito à Portabilidade tanto os dados pessoais diretamente fornecidos pelo titular, como aqueles que são observados pelo responsável pelo tratamento em virtude da utilização de determinado produto, serviço ou dispositivo pelo titular dos dados.

Neste cenário, se um determinado utilizador criar uma conta num *website* que presta serviços de *streaming* de filmes e séries, os dados diretamente fornecidos poderão ser o nome, número

[27] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation …*; 164 e ss.; Peter Carey, *Data Protection…*, 147 e ss; "Guide to the General Data Protection Regulation", Information Commissioner's Office, acesso em 20 de abril de 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/; Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, *The Standard Data Protection Model …*, 20 e ss.

[28] "Orientações sobre o direito à portabilidade dos dados", GT29, acesso em 15 de abril de 2020, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

do cartão de crédito, idade, géneros preferidos etc. Quanto aos dados observados poderão incluir, por exemplo, os filmes e séries vistos ou que o utilizador tenha assinalado como planeando ver no futuro.
No entanto, o Direito à Portabilidade não abrange os dados "inferidos" e os dados "derivados". Estes são dados que são obtidos pelo responsável pelo tratamento, após tratar os dados diretamente fornecidos ou observados. O fornecimento deste tipo de dados poderia colocar em jogo a liberdade de iniciativa económica dos responsáveis pelo tratamento e um conjunto de direitos associados como os segredos de negócio. Imagine-se que, para além de ter de fornecer os dados acima referidos, a plataforma tivesse também de fornecer o perfil de utilizador no qual enquadrou o titular dos dados e, eventualmente, as sugestões associadas a este perfil e escolhas do utilizador. Desta forma, um concorrente que não tivesse feito um investimento tão avultado num algoritmo sofisticado para sugestão de novas escolhas poderia aproveitar este trabalho através da portabilidade ou mesmo, com base em técnicas de *reverse engineering,* ser capaz de reproduzir a ferramenta utilizada pela primeira plataforma.

O Direito à Portabilidade implica que o titular dos dados tenha o direito a receber os seus dados num formato estruturado, de uso corrente e de leitura automática[29] e/ou de transferir estes dados para outro responsável pelo tratamento. Quando tecnicamente possível, esta transferência deve ser direta (entre responsáveis pelo tratamento), de forma a assegurar a manutenção da proteção dos dados do titular ou de terceiros[30].

De referir que, no contexto da *European Strategy for Data*, a Comissão Europeia lançou a discussão sobre uma eventual expansão do Direito à Portabilidade considerando que *"[i]mporta continuar a apoiar as pessoas no exercício dos direitos relativos à utilização dos dados por si gerados. Para controlarem os seus dados, poderão recorrer a instrumentos e meios que lhes permitam decidir, com grande nível de pormenor, o que é feito com os seus dados («espaços de dados pessoais»). O reforço do direito de portabilidade previsto no artigo 20.º do RGPD poderá contribuir para alcançar este objetivo, conferindo às pessoas mais controlo sobre quem pode aceder e utilizar dados gerados automaticamente, nomeadamente aplicando requisitos mais rigorosos às interfaces de acesso aos dados em tempo real e tornando obrigatórios os formatos legíveis por máquina para os dados de determinados produtos e serviços, por exemplo, os dados provenientes de eletrodomésticos inteligentes ou de tecnologias usáveis. Além disso, podem ser equacionadas regras aplicáveis aos fornecedores de aplicações que envolvam dados pessoais ou a novos intermediários de dados, como os fornecedores de espaços de dados pessoais, garantindo o seu papel como intermediários neutros"*[31].

[29] O Considerando 68 refere que o dito formato deve ser, igualmente, interoperável.
[30] "Orientações sobre o direito à portabilidade dos dados", GT29, acesso em 15 de abril de 2020, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233; Rita de Sousa Costa, *"O direito à portabilidade dos dados pela lente do direito da concorrência: breve relance em contagem decrescente para a aplicação do Regulamento Geral sobre a Proteção de Dados"*, Revista de Concorrência e Regulação, 33/34 (2018): 291-299.
[31] Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: A European strategy for data, Comissão Europeia, acesso a 20 de abril de 2020, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

2.7. Direito de Oposição

Nos termos do artigo 21.º, n.º 1 do RGPD, "o titular dos dados terá o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular", ao tratamento dos dados pessoais que lhe digam respeito, quando a base legal para a respetiva operação de tratamento seja: a) os interesses legítimos do responsável pelo tratamento ou de terceiros [artigo 6.º, n.º 1, al f) do RGPD] ou b) o interesse público [artigo 6.º, n.º 1, al e) do RGPD]. O titular dos dados pode ainda fazer uso do Direito de Oposição quando o tratamento tenha como base o artigo 6.º, n.º 4 do RGPD[32].

Quando haja oposição do titular dos dados, o responsável pelo tratamento apenas poderá prosseguir as suas operações de tratamento caso apresente (e comprove) a existência de razões imperiosas e legítimas que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados. Alternativamente, os dados poderão continuar a ser tratados quando sejam necessários para efeitos de declaração, exercício ou defesa de um direito num processo judicial (e exclusivamente para este efeito).

Uma questão que pode surgir no contexto do Direito de Oposição é a de saber se este direito pode ser exercido quando se esteja perante operações de tratamento que envolvam categorias especiais de dados, uma vez que tal não se encontra claro no RGPD.

Todavia, resulta hoje pacífico que o tratamento de categorias especiais de dados exige um duplo fundamento de licitude: i) um fundamento de licitude do artigo 6.º do RGPD e ii) um fundamento de licitude do artigo 9.º do RGPD[33]. Deste modo, o Direito de Oposição relativamente ao tratamento de dados especiais poderá ser invocado quando o fundamento de licitude, nos termos do artigo 6.º do RGPD, coincidir com um dos fundamentos referidos no artigo 21.º, n.º 1 do RGPD.

Uma interpretação diversa, à luz das considerações anteriores, não só entraria em contradição com a necessidade de duplo fundamento de licitude como, potencialmente, colocaria as

[32] Quando o responsável, com base no teste de compatibilidade prescrito neste mesmo artigo, leve a cabo: a) um "tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos" e b) este tratamento não for "realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos" no artigo 23.º, n.º 1 do RGPD.

[33] Como bem notou o Comité Europeu de Proteção de Dados em diversas ocasiões. Cfr. "Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation", Comité Europeu de Proteção de Dados, acesso em 20 de abril de 2020, https://edpb.europa.eu/our-work-tools/our-documents/avis-art-70/opinion-32019-concerning-questions-and-answers-interplay_en; "Guidelines 3/2019 on processing of personal data through video devices", Comité Europeu de Proteção de Dados, acesso em 20 de abril de 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en; Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, Comité Europeu de Proteção de Dados, acesso em 21 de abril de 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en. Adicionalmente, "Guide to the General Data Protection Regulation", Information Commissioner's Office, acesso em 20 de abril de 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/; "Guidance Note: Legal Bases for Processing Personal Data", Data Protection Commission, acesso em 20 de abril de 2020, https://www.dataprotection.ie/sites/default/files/uploads/2019-12/Guidance%20on%20Legal%20Bases_Dec19_1.pdf; Health-related personal data – regarding COVID-19 and digital surveillance", Alessandra Silveira, acesso em 20 de abril de 2020, https://officialblogofunio.com/2020/04/01/editorial-of-march-2020-2/; Acórdão do TJUE de 6 de novembro de 2003, *Lindqvist*, Processo C-101/01, ECLI:EU:C:2003:596.

categorias especiais de dados, mais sensíveis e tradicionalmente mais protegidas, numa situação de menor proteção que o "comum" dos dados pessoais.

2.8. Direito a Não Ficar Sujeito a Decisões Individuais Automatizadas

Nos termos do artigo 22.º, n.º 1 do RGPD, o titular dos dados tem o direito a não ficar sujeito *"a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar".*

Esta proibição geral não se aplica quando o tratamento de dados, através de decisão individual automatizada *a)* seja necessário para a celebração ou execução de um contrato entre o responsável pelo tratamento e o titular dos dados; *b)* for autorizado pelo direito da União Europeia ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; *c)* for baseado no consentimento explícito do titular dos dados (artigo 22.º, n.º 2 do RGPD).

Por sua vez, o artigo 22.º, n.º 3 do RGPD estabelece que "*[n]os casos a que se referem o n.º 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão*".

Posto isto, o Considerando 71, que serve como ferramenta interpretativa às normas deste dispositivo, esclarece que: "*a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento (…), ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão".*

Assim, enquanto o Considerando 71 sugere uma aplicação geral ("[e]m qualquer dos casos") de medidas adequadas, o artigo 22.º, n.º 3 do RGPD parece diferenciar tais medidas consoante o tratamento tenha como base *i)* o consentimento [nos termos da alínea c) do n.º 2] ou a celebração/execução de contrato [nos termos da alínea a) do n.º 2] ou *ii)* uma autorização legal [nos termos da alínea b) do n.º 2]. Daqui deriva a seguinte questão: o direito de obter intervenção humana, manifestar o seu ponto de vista e contestar a decisão deve ser considerado um mínimo universal relativamente às decisões individuais automatizadas, ou seria apenas aplicável aos fundamentos distintos da autorização legal?

Se, por um lado, a distinção feita no próprio artigo poderia indiciar uma vontade do legislador em não estabelecer tais requisitos mínimos quando estivesse em causa uma autorização legal, há ponderosas razões de caráter jusfundamental para concluir-se o contrário. Não sendo o Considerando 71 contraditório face ao espírito do artigo 22.º do RGPD, não parece existir uma

razão atendível para submeter os tratamentos baseados em autorização legal a um *standard* menos elevado em relação a outros tipos de tratamento, pois só assim o padrão de jusfundamentalidade prosseguido pela União Europeia no que tange à proteção de dados pessoais poderá ser atingido (artigo 8.º da Carta dos Direitos Fundamentais da União Europeia).

Importa ainda incidir no conceito de decisão tomada exclusivamente com base no tratamento automatizado. Para que se considere que uma decisão não se enquadra neste conceito, será necessário que exista uma intervenção humana relevante. Isto é, a pessoa que supervisione a "máquina" deverá ter a autoridade e competência (funcional e técnica) necessária para alterar a decisão em causa. Naturalmente, a pessoa encarregada de supervisionar a "máquina" deve ter a capacidade de detetar erros, estar razoavelmente familiarizada com o programa e ser diligente[34].

De qualquer forma, a proibição geral apenas se aplica quando o tratamento produz efeitos na esfera jurídica do titular dos dados ou o afete significativamente de forma similar[35]. Aferir o preenchimento de tais conceitos indeterminados pode colocar desafios interpretativos que demandem o "diálogo de juiz a juiz", com o TJUE, através do reenvio prejudicial[36].

3. Notas conclusivas

A natureza deste texto não é compatível com conclusões particularmente densas, pelo que se deixam apenas algumas pistas sobre a aplicação das normas do RGPD pelos Tribunais quanto aos direitos dos titulares dos dados referidos *supra*.

Em primeiro lugar, é de referir que o TJUE tende a interpretar as normas relativas à proteção de dados pessoais de forma pragmática e evitando desproteger o titular dos dados perante fenómenos que não tenham sido previstos aquando da elaboração dos diplomas que regulam tais matérias. Tal era frequente com a Diretiva 95/46/CE e não deverá mudar com o RGPD.

Adicionalmente, em caso de dúvida sobre a interpretação das normas do RGPD – o que poderá acontecer com alguma frequência dada a especificidade do diploma e a necessidade de interpretação principiológica que o caracteriza –, o reenvio prejudicial para o TJUE deverá ser acionado imediatamente, a fim de evitar a aplicação equivocada de tais normas na UE. As características do RGPD fazem com que o seu sucesso ou insucesso como ferramenta legal

[34] Critério idêntico deverá aplicar-se relativamente à pessoa que for chamada a rever as decisões da "máquina" caso o titular dos dados exerça o seu direito de obter intervenção humana. Adicionalmente, o revisor deve ter em conta não só toda a informação relevante que possuía *ex ante*, como também toda a informação relevante que lhe seja facultada pelo titular dos dados. Logicamente, o revisor deve ter também o poder de reverter a decisão originariamente tomada.

[35] Em língua inglesa *"which produces legal effects concerning him or her or similarly significantly affects him or her"*. Para um maior desenvolvimento dos conceitos gerais analisados nesta secção, e dada a existência de limitações de espaço ao presente trabalho, *vd.* Tiago Sérgio Cabral, *AI Regulation in the European Union: …*, 179 e ss; "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", GT29, acesso em 5 de abril, 2020; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[36] Para uma análise mais profunda desta questão, *vd.* Tiago Sérgio Cabral, "AI and the Right to Explanation: Three Legal Bases under the GDPR", in *Computers, Privacy & Data Protection 2020* (Oxford: Hart Publishing, 2020), no prelo.

esteja dependente da sua efetiva aplicação uniforme, tendo os Tribunais um papel de particular relevância para a sua consecução. Deste modo evitam-se também situações indesejáveis como potenciais tentativas de responsabilização do Estado por violação do RGPD ou mesmo ações por incumprimento, contra o Estado português, por parte da Comissão Europeia (cuja iniciativa pode ser despoletada por queixa apresentada por um particular).

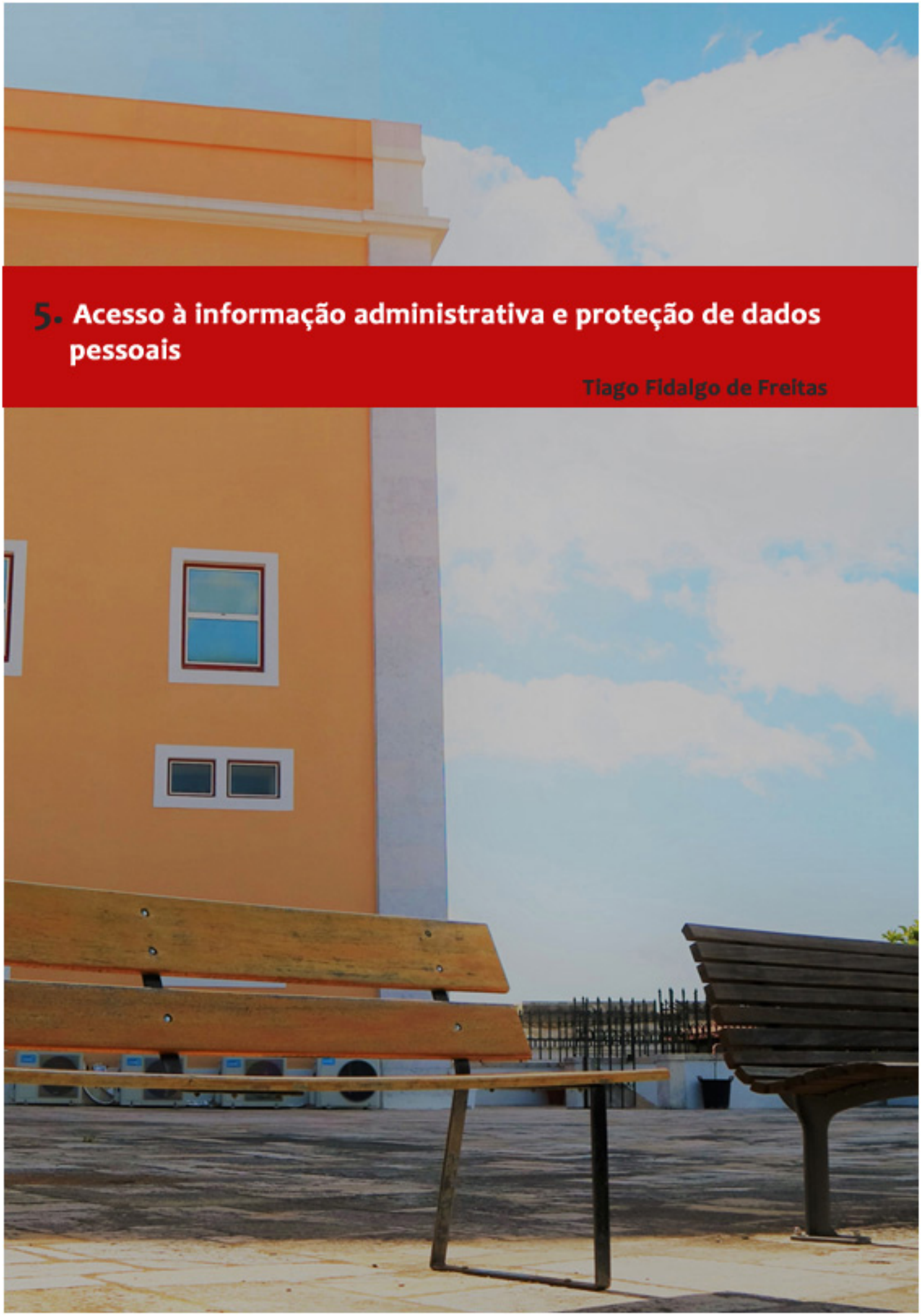
Nesta linha, e ainda na tónica jurisdicional do RGPD, verificamos que este atribui aos Tribunais um poder de fiscalização independente cuja utilização se revela essencial. Afinal, quando operam no âmbito de aplicação do direito da União (como é evidente no caso da proteção de dados), os Tribunais estariam melhor apetrechados a promover uma tutela mais efetiva dos direitos dos titulares dos dados, na medida em que têm, à sua disposição, o mecanismo do reenvio prejudicial, tendente a aferir o sentido e o alcance das normas do RGPD. Posto isto, o próprio sistema de aplicação do direito da União faz impender sobre os juízes nacionais – enquanto juízes funcionalmente europeus – uma tarefa catártica que nem mesmo as autoridades de controlo dos Estados-Membros poderão assegurar, basicamente por não gozarem de equivalente instrumento de aferição da interpretação do direito da União.

Deste modo, para a salvaguarda dos direitos conferidos no âmbito do RGPD, há uma dinâmica trimembre sem a qual a efetividade do direito da União poderá perigar – qual seja, aquele ato normativo europeu demanda uma interpretação em conformidade que se impõe, de igual modo, às autoridades de controlo e aos Tribunais nacionais, cabendo aos últimos a interação reflexiva com o TJUE. Só assim se promove a aplicação correta do RGPD tanto na esfera jurídica dos titulares dos dados como na dos responsáveis pelo tratamento.

Por fim, importa atentar nas limitações impostas ao legislador nacional em matéria de proteção de dados e aferir em que medida este estaria porventura a extravasar as suas competências quando surjam normas nacionais integráveis no âmbito de aplicação do RGPD. Nestas situações, os Tribunais nacionais devem perceber se é possível interpretar a norma nacional em conformidade com o direito da União ou se o seu afastamento é a solução que se impõe. Novamente aqui o reenvio prejudicial será a melhor forma para aferir qual das soluções será equacionável para o caso concreto.

Vídeo da apresentação

https://educast.fccn.pt/vod/clips/ey9r3rrzg/ipod.m4v?locale=pt



5. Acesso à informação administrativa e proteção de dados pessoais

Tiago Fidalgo de Freitas

CENTRO
DE ESTUDOS
JUDICIÁRIOS

5. AS RESTRIÇÕES AO DIREITO À INFORMAÇÃO ADMINISTRATIVA COM FUNDAMENTO NA PROTEÇÃO DE DADOS PESSOAIS: ALGUMAS NOTAS[*]

Tiago Fidalgo de Freitas[**]

Vídeo

1. A intimação para a prestação de informações, consulta de processos ou passagem de certidões encontra-se estruturada como instrumento específico de tutela jurisdicional do direito fundamental à informação administrativa – procedimental e não procedimental[1]. Não surpreende, por isso, que para as suas exata delimitação e compreensão seja essencial conhecer o âmbito de proteção destes últimos direitos fundamentais.

O presente artigo visa dar um contributo, ainda que sumário, para essa análise, focando-se especificamente numa das (várias) restrições legalmente previstas aos referidos direitos à luz do direito hoje em vigor e que implica a conjugação de normas europeias e nacionais, quer constitucionais, quer legais. Trata-se, em concreto, do direito à proteção de dados pessoais, decorrência do direito à reserva da intimidade da vida privada, que constitui outro direito fundamental internacional e constitucionalmente protegido.

Daqui se retira, portanto, que outros temas de ordem geral a propósito da transparência administrativa e do acesso à informação administrativa – quer tenham implicações substantivas, implicações processuais ou ambas – que extravasem esta questão muito específica estão, por isso, excluídos do seu objeto[2].

2. A definição do âmbito objetivo do direito à divulgação de informação é, à partida, marcada pela imposição geral de um dever de divulgação de toda a informação necessária aos requerentes[3]. Trata-se, porém, e ao contrário do que se poderia intuir, de um mero dever *prima facie*, porque ainda tem de ser ponderado e sopesado com outros bens constitucionais

[*] Apresentação decorrente da ação de formação contínua do CEJ "Proteção de Dados Pessoais", realizada a 19 de junho de 2019.

[**] Assistente convidado da Faculdade de Direito da Universidade de Lisboa; investigador associado e coordenador executivo do CIDP – Centro de Investigação de Direito Público; consultor coordenador do Centro de Competências Jurídicas do Estado (JurisAPP).

[1] Cfr. artigo 104.º, n.º 1, do Código de Processo nos Tribunais Administrativos.

[2] Para um enquadramento geral e abrangente sobre o tema, cfr. T. FIDALGO DE FREITAS, 'O acesso à informação administrativa: regime e balanço', in T. FIDALGO DE FREITAS / P. DELGADO ALVES (org.), *O acesso à informação administrativa*, Coimbra: Almedina, 2021 (no prelo); ID., 'A dimensão constitucional da transparência', in R. LOBO XAVIER *et al.* (eds.), *Constitucionalismos e (con)temporaneidade. Homenagem ao Prof. Doutor Manuel Afonso Vaz*, Lisboa: UCE, 2020, pp. 207-233; ID., 'Administrative transparency in Portugal', European Public Law, vol. 22, n.º 4, 2016, pp. 667-688.

[3] Mesmo assim, ainda se encontram atualmente exemplos flagrantes de atos manifestamente inconstitucionais e ilegais por violação deste dever – o que é verdadeiramente incompreensível. É o caso, por exemplo, do Despacho n.º 1612-A/2017, do Secretário de Estado da Saúde, publicado no *Diário da República*, n.º 35, 1.º Suplemento, Série II, de 17 de fevereiro de 2017, nos termos do qual "Os serviços e organismos integrados na administração direta e indireta do Estado, no âmbito do Ministério da Saúde, e das entidades do setor público empresarial, da área da saúde, não podem ceder a entidades privadas, a título gratuito ou oneroso, dados estatísticos sobre produção e consumos, sem prévia autorização do membro do Governo responsável pela área da saúde". Nem o despacho que o revogou – tendo dispensado "da autorização prévia do membro do governo responsável pela área da saúde, a transferência de dados para entidades terceiras, que se encontre devidamente justificada e fundamentada, no âmbito de protocolos de investigação ou da realização de análises ou estudos solicitados pelos próprios serviços ou instituições do Serviço Nacional de Saúde (SNS) e desde que não envolva a transferência de dados pessoais identificados ou identificáveis" – escapa das referidas inconstitucionalidade e ilegalidade – cfr. Despacho n.º 4354-A/2017, do Secretário de Estado da Saúde, publicado no *Diário da República*, n.º 97, 1.º Suplemento, Série II, de 19 de maio de 2017.

relevantes. Ou seja: as normas que estabelecem o dever de providenciar a informação renunciam à possibilidade de regular de forma definitiva a situação por si próprias e expõem-se ao peso de todos os interesses privados e públicos de sentido convergente e/ou contrário, interesses esses que deverão ser avaliados pelo órgão administrativo competente casuisticamente[4]. O direito de acesso não é, por isso, absoluto – da mesma forma que tão-pouco as exceções ao mesmo o são.

3. Ao nível constitucional[5], o enunciado normativo correspondente à norma que atribui o direito fundamental de acesso à informação administrativa procedimental poderia, contudo, gerar perplexidades. Isto porque, ao contrário da norma que atribui o direito fundamental de acesso à informação administrativa não procedimental – que se aplica "sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal e à intimidade das pessoas"[6] –, aqueloutra norma está constitucionalmente plasmada sem qualquer exceção. Poder-se-ia retirar dessa ausência de previsão de exceções, especialmente por contraste com o direito de acesso aos arquivos, que não haveria lugar a qualquer ponderação.

Não é, contudo, assim. Apesar da aparente ausência de autorização constitucional explícita[7], parece inequívoco que o direito à informação administrativa procedimental pode ser restringido por meio de ato legislativo[8], visto que as normas de direitos (fundamentais) têm uma natureza de norma-princípio e estão sujeitas a um mandato de otimização, designadamente com outras normas-princípios constitucionais[9/10]. O fundamento não pode

[4] Considerando também que as decisões são tomadas casuisticamente, de acordo com o resultado da ponderação feita em cada caso de conflito de direitos ou bens constitucionais, cfr. J. E. FIGUEIREDO DIAS, 'Direito à informação, proteção da intimidade e autoridades administrativas independentes', in AA.VV., *Estudos em homenagem ao Prof. Doutor Rogério Soares*, Coimbra: Coimbra Editora, 2001, p. 639. Sublinhando que a ponderação ocorre mesmo no caso do (atual) artigo 83.º do Código do Procedimento Administrativo, cfr. F. PAES MARQUES, *As relações jurídicas administrativas multipolares*, Coimbra: Almedina, 2011, pp. 381-382. Falando de áreas excecionadas de forma não definitiva e sujeita a ponderação *ad hoc*, cfr. M. AROSO DE ALMEIDA, 'Os direitos fundamentais dos administrados após a revisão constitucional de 1989', Direito e Justiça, n.º 6, 1992, pp. 315-316. Por esta razão, é muito duvidoso afirmar que o ato de divulgar informações seja não discricionário, como entendem S. DAVID, *Das intimações*, Coimbra: Almedina, 2005, pp. 190-192, e A. BRANDÃO DA VEIGA, *Acesso à informação da administração pública pelos particulares*, Coimbra: Almedina, 2007, pp. 240-241 (que, no entanto, considera noutro ponto que a ponderação é um problema sistémico central da divulgação de informações administrativas – cfr. pp. 183-191). Em geral sobre a ponderação no direito administrativo, cfr. P. OTERO, *Manual de direito administrativo*, I, Coimbra: Almedina, 2013, pp. 432-449; D. DUARTE, *A norma de legalidade procedimental administrativa*, Coimbra: Almedina, 2006, pp. 565-575.

[5] Da perspetiva constitucional, cfr. T. FIDALGO DE FREITAS, 'A dimensão constitucional da transparência', in R. LOBO XAVIER *et al.* (eds.), *Constitucionalismos e (con)temporaneidade. Homenagem ao Prof. Doutor Manuel Afonso Vaz*, Lisboa: UCE, 2020, pp. 227-233.

[6] Cfr. artigo 268.º, n.^{os} 1 e 2, da Constituição.

[7] Aparentemente exigida pelo artigo 18.º, n.º 2, da Constituição, ao determinar que "A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição […]". Para uma análise desenvolvida das diferentes posições existentes na doutrina nacional no que à interpretação da primeira parte do artigo 18.º, n.º 2, da Constituição, cfr. J. DE MELO ALEXANDRINO, *A estruturação do sistema de direitos, liberdades e garantias na Constituição portuguesa*, II, Coimbra: Almedina, 2006, pp. 443-457; posteriormente, cfr. J. PEREIRA DA SILVA, *Direitos fundamentais. Teoria geral*, Lisboa: Universidade Católica Editora, 2018, pp. 237-249.

[8] De forma semelhante, cfr. J. MIRANDA, 'O direito de informação dos administrados', O Direito, n.º 120/III-IV, 1988, pp. 461-462; A. RODRIGUES QUEIRÓ, 'Anotação ao Acórdão do Supremo Tribunal Administrativo (1.ª Secção) de 22 de janeiro de 1981', Revista de Legislação e Jurisprudência, n.º 114, 1981-1982, pp. 308-309. De forma matizada, cfr. J. C. VIEIRA DE ANDRADE, *Os direitos fundamentais na Constituição portuguesa de 1976*[5], Coimbra: Almedina, 2012, pp. 277-281; contra, M. A. VAZ, *Lei e reserva da lei: a causa da lei na Constituição portuguesa de 1976*, Porto: Universidade Católica Portuguesa, 1992, pp. 323-332.

[9] Sobre direitos (fundamentais) *prima facie* e ponderação, cfr. J. REIS NOVAIS, *Direitos fundamentais e justiça constitucional*, Lisboa: AAFDL, 2017, pp. 69-99; ID., *As restrições aos direitos fundamentais não expressamente autorizadas pela Constituição*, Coimbra: Coimbra Editora, 2003, *per totum*, em especial pp. 322-353, 693-725; M. L.

ser, assim, a alegada proximidade entre os dois direitos, o que resultaria na aplicação das restrições constitucionalmente previstas para o primeiro também ao segundo direito fundamental, ao contrário do que o Tribunal Constitucional considerou em decisões anteriores[11]. Aliás, e por absurdo, se esse argumento fosse válido, o mesmo equivaleria a defender que, antes da revisão constitucional de 1989, quando o direito à informação não instrumental não estava previsto no texto constitucional, não era possível restringir o direito à informação procedimental.

4. Ao nível da lei ordinária, deve entender-se que os fundamentos com base nos quais o órgão responsável pela direção do procedimento está especificamente autorizado a ponderar a concessão de acesso à informação administrativa, tanto procedimental quanto não procedimental – no sentido de poder recusá-la –, são delimitados de acordo com o conteúdo da informação em causa. E, contrariamente ao que seria expectável (e desejável), os motivos que a lei explicitamente admite que sejam usados como fundamento de decisões de indeferimento dos pedidos de acesso à informação não são comuns aos dois tipos de direitos – de facto, pelo menos de acordo a letra da lei, só se sobrepõem parcialmente no âmbito dos dois direitos em análise.

5. Deverá começar-se por notar que toda e qualquer restrição ao acesso à informação administrativa fundada em motivos de interesse privado só é aplicada em casos de pedidos de terceiros. Cada pessoa tem, assim, acesso completo às informações que lhe digam diretamente respeito[12] – daí que, por exemplo, seja lícito o acesso à gravação de uma

---

AMARAL, *A forma da república. Uma introdução ao estudo do direito constitucional*, Coimbra: Coimbra Editora, 2005, pp. 102-109. Cfr. também, embora em sentido não inteiramente coincidente (nem entre si, nem com a posição anteriormente citada), P. MONIZ LOPES, 'The syntax of principles: genericity as a logical distinction between rules and principles', Ratio Juris, vol. 30, n.º 4, 2017, pp. 471-490; ID., *Derrotabilidade normativa e normas administrativas. O enquadramento das normas regulamentares na teoria dos conflitos normativos*, I, Lisboa: AAFDL, 2019, pp. 157-198; D. DUARTE, *A norma de legalidade procedimental administrativa*, pp. 727-754, 761-797. Em sentido crítico sobre alguns aspetos da distinção entre regras e princípios, cfr. C. BLANCO DE MORAIS, *Curso de direito constitucional*, II[2], Coimbra: Almedina, 2018, pp. 516-534.

[10] O Tribunal Constitucional veio a adotar uma linha de decisão que não se afasta muito desta no seu Acórdão n.º 254/99, também sobre acesso à informação administrativa, como salientam J. MIRANDA / J. DE MELO ALEXANDRINO, 'As grandes decisões dos Tribunais Constitucionais europeus. Portugal', pp. 13-17, disponível em URL: https://bit.ly/36G8TqE. Depois, cfr., por exemplo, o Acórdão do Tribunal Constitucional n.º 136/2005.

[11] Isto mesmo foi defendido pelo Tribunal Constitucional nos seus Acórdãos n.[os] 176/92 e 177/92. Considerando este argumento "metodologicamente insustentável", e com razão, cfr. a crítica contundente de J. J. GOMES CANOTILHO, 'Anotação aos Acórdãos do Tribunal Constitucional n.[os] 176/92 e 177/92', Revista de Legislação e Jurisprudência, n.º 125, 1992-1993, p. 254. Cfr. também P. MACHETE, *A audiência dos interessados no procedimento administrativo*, Lisboa: Universidade Católica Editora, 1995, pp. 404-405[847].

[12] A lei previa, não obstante, uma exceção: a parte interessada em obter informação sobre a sua própria saúde (em particular, o seu processo clínico) podia ter o seu pedido de acesso negado "em circunstâncias excecionais, devidamente justificadas, e nas quais [tenha sido] inequivocamente demonstrado que estas podem ser danosas para o interessado" – cfr. artigo 3.º, n.º 2, da Lei n.º 12/2005, de 26 de janeiro, que aprovou a lei sobre informação genética pessoal e informação de saúde, foi alterada pela Lei n.º 26/2016, de 22 de agosto, e foi regulamentada pelo Decreto-Lei n.º 131/2014, de 29 de agosto, que aprovou o regime jurídico da proteção e confidencialidade da informação genética. Constituía o chamado 'privilégio terapêutico', como dá nota S. PRATAS, *O acesso à informação de saúde*, Vila de Rei: Caminhos de Pax, 2015, p. 75. Tratava-se de uma norma de muito duvidosa constitucionalidade – também neste sentido, cfr. termos semelhantes, cfr. A. SOUSA PINHEIRO, Privacy *e proteção de dados: a construção dogmática do direito à identidade informacional*, dissertação de doutoramento, Lisboa: s.n., 2012, pp. 881-887, 894-896; diferentemente, C. BARBOSA, 'Questões jurídicas do acesso ao processo clínico', Lex Medicinae, ano 7, n.º 13, 2010, p. 115, considerava que os únicos dados aos quais os pacientes podiam ter o acesso negado eram as anotações pessoais do médico contidas no arquivo; ao contrário do que defendia C. BARBOSA, *idem*, pp. 116-119, a lei em causa não foi revogada. Ambas estas leis encontram-se compiladas em F. PAES MARQUES / T. FIDALGO DE FREITAS (orgs.), *Legislação de proteção de dados*, Lisboa: AAFDL, 2019, pp. 415-448.

chamada telefónica feita pelo próprio requerente para um serviço público cujas chamadas são gravadas por determinação legal[13].

6. No que à privacidade e à proteção de dados pessoais concerne, existem duas questões por resolver:

> (a) Uma questão *substantiva*, que consiste em determinar qual o regime material aplicável aos documentos que contenham dados pessoais que estejam na posse de uma das entidades sujeitas ao âmbito de aplicação da Lei de Acesso aos Documentos Administrativos: será o regime desta lei ou o regime do Regulamento Geral sobre Proteção de Dados?
> (b) Uma questão *orgânico-regulatória*, que consiste em saber que entidade é competente para fazer o controlo do acesso a esses mesmos documentos por terceiros: a Comissão de Acesso aos Documentos Administrativos – que é a "entidade administrativa independentente a quem cabe zelar pelo cumprimento das disposições" da Lei de Acesso aos Documentos Administrativos[14] – ou a Comissão Nacional de Proteção de Dados – que é a "autoridade de controlo nacional para efeitos do Regulamento Geral de Proteção de Dados", sendo que "controla e fiscaliza […] [as] disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos de dados pessoais"[15]?

Apesar de distintas, as duas problemáticas encontram-se indissociavelmente ligadas pela evolução do quadro legislativo aplicável – marcada, no essencial, pela renúncia do legislador nacional à resolução definitiva, tanto quanto possível, da questão[16] – e pela história do diálogo regulatório (ou da falta dele) entre a Comissão de Acesso aos Documentos Administrativos e a Comissão Nacional de Proteção de Dados. Durante largos anos, a "intersecção regulatória"[17] entre estes órgãos foi problemática, verificando-se um conflito positivo de competências quanto a questões relativas ao acesso, ou à recusa de acesso, a documentos administrativos

[13] Cfr. Parecer da Comissão de Acesso aos Documentos Administrativos n.º 144/2019.
[14] Cfr. artigos 28.º a 37.º da Lei de Acesso aos Documentos Administrativos. Para mais desenvolvimentos sobre a Comissão de Acesso aos Documentos Administrativos, cfr. *infra*.
[15] Cfr. artigo 2.º, n.os 2 e 3, da Lei de Organização e Funcionamento da Comissão Nacional de Proteção de Dados, aprovada pela Lei n.º 43/2004, de 18 de agosto, alterada pela Lei n.º 55-A/2010, de 31 de dezembro, e pela Lei n.º 58/2019, de 8 de agosto – coligida e consolidada em F. PAES MARQUES / T. FIDALGO DE FREITAS (orgs.), *Legislação de proteção de dados*, pp. 187-203. A Comissão Nacional de Proteção de Dados está prevista no artigo 35.º, n.º 2, da Constituição, e foi pela primeira vez instituída pela Lei n.º 10/91, de 29 de abril, mais tarde alterada pela Lei n.º 28/94, de 29 de agosto. Trata-se, também ela, de uma entidade administrativa independente – para mais referências, cfr. F. PEREIRA COUTINHO, 'A independência da Comissão Nacional de Proteção de Dados', Anuário da Proteção de Dados, 2020, pp. 14-47; F. URBANO CALVÃO, 'Garantia de direitos: a proteção dos dados pessoais perante os desafios tecnológicos', in C. AMADO GOMES *et al.* (coord.), *Garantia de direitos e regulação: perspetivas de direito administrativo*, Lisboa: AAFDL, 2020, pp. 186-204; ID., 'O RGPD e o papel da Comissão Nacional de Proteção de Dados', Revista de Direito Administrativo, n.º 4, janeiro-julho 2019, pp. 68-70; A. SOUSA PINHEIRO, Privacy *e protecção de dados*, pp. 863-868; J. L. CARDOSO, *Autoridades administrativas independentes e Constituição*, Coimbra: Coimbra Editora, 2002, pp. 315-330; A. GUERRA, 'A lei de proteção de dados pessoais', in AA.VV., *Direito da sociedade da informação*, II, Coimbra: Coimbra Editora, 2001, pp. 151-154.
[16] Também assim, mas especificamente quanto às soluções do Código do Procedimento Administrativo, cfr. M. ASSIS RAIMUNDO, 'Os princípios no novo CPA e o princípio da boa administração, em particular', in C. AMADO GOMES *et al.* (coord.), *Comentários ao novo Código do Procedimento Administrativo*[2], Lisboa: AAFDL, 2015, pp. 180-181.
[17] Na expressão feliz de F. PAES MARQUES, 'Acesso à informação administrativa e proteção de dados', in C. AMADO GOMES *et al.* (coord.), *Garantia de direitos e regulação*, p. 261.

que contivessem dados pessoais. Antagonismo esse que era significativamente ampliado pelo facto de ambas as entidades utilizarem terminologias muito técnicas – designadamente em matéria de proteção de dados – que, ao tempo, não eram imediatamente apreensíveis por quem não estivesse iniciado nessa área científica.

Seja como for, nessa disputa, crê-se que a razão não estava inteiramente de nenhum dos lados. De facto, se a Comissão Nacional de Proteção de Dados tinha uma visão de monopólio natural, exclusivamente a seu cargo, de todos e quaisquer temas relacionados com dados pessoais[18], bem como uma visão absoluta e intangível do direito à proteção de dados pessoais, a Comissão de Acesso aos Documentos Administrativos ignorava que o acesso a documentos administrativos constituía uma forma de tratamento de dados pessoais[19]. Não obstante, não se vai, aqui e agora, retomar os termos dessa querela em perspetiva histórica. Interessa apenas apontar aqueles que se consideram ser os termos adequados da sua resolução à luz das normas atualmente em vigor.

7. Considera-se, em primeiro lugar, que é legítimo que o legislador nacional aprove um regime material específico para o acesso a documentos administrativos que contenham dados pessoais – que é, no caso, o constante da Lei de Acesso aos Documentos Administrativos[20] – por força das seguintes razões:

(i) A Constituição consagra, como direitos fundamentais autónomos, tanto o direito à privacidade[21] quanto o direito à proteção de dados pessoais[22/23] – o que significa,

[18] Cfr. Deliberação da Comissão Nacional de Proteção de Dados n.º 241/2014 – em que sugeriu à Assembleia da República, *sponte sua*, a revisão da Lei de Acesso aos Documentos Administrativos de 2007 – e Pareceres da Comissão Nacional de Proteção de Dados n.os 24/2015 – a pedido da Assembleia da República sobre uma proposta de lei que não chegou a ser aprovada – 6/2016 e 11/2016 – a pedido, respetivamente, do Governo e da Assembleia da República, no âmbito do procedimento legislativo de aprovação da Lei de Acesso aos Documentos Administrativos de 2016 – e, por fim, 20/2018 – a pedido também da Assembleia da República no âmbito do procedimento legislativo de aprovação da Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento Geral sobre a Proteção de Dados. A posição da Comissão Nacional de Proteção de Dados tem-se alicerçado nos argumentos de que o regime da Lei de Acesso aos Documentos Administrativos, ao contrário do que resultaria do Regulamento Geral sobre a Proteção de Dados: (i) não ofereceria aos titulares de dados pessoais contidos em documentos administrativos nominativos as mesmas garantias substantivas de acesso aos seus próprios dados, o que ofenderia o princípio da igualdade; (ii) seria menos protetora quanto ao acesso por terceiros a dados pessoais, estabelecendo a liberdade de acesso, sem necessidade de invocar qualquer interesse, ao contrário do que resultaria do princípio da finalidade, o que violaria não só esse mesmo princípio, mas também o princípio da igualdade e ainda o artigo 35.º, n.º 4, da Constituição; (iii) o titular de dados pessoais contidos em documentos administrativos não poderia recorrer a uma entidade administrativa independente dotada de autotutela executiva e declarativa, com poderes inspetivos e corretivos, em contradição com o que decorreria do artigo 35.º, n.º 2, da Constituição e esvaziando as competências da Comissão Nacional de Proteção de Dados; (iv) inexistiriam garantias de não reutilização de documentos que contêm dados pessoais e de não reversibilidade da anonimização; (v) verificar-se-ia, em suma, uma violação do direito da União Europeia relevante – inicialmente das Diretivas n.os 95/46/CE e 2003/98/CE, atualmente do Regulamento Geral sobre a Proteção de Dados, e em qualquer caso do artigo 8.º da Carta dos Direitos Fundamentais da União Europeia.

[19] Cfr., designadamente, Pareceres da Comissão de Acesso aos Documentos Administrativos n.os 118/2002, 132/2014, 170/2015 e 64/2016.

[20] Ao contrário do que entende a Comissão Nacional de Proteção de Dados, que, no seu Parecer n.º 20/2018, p. 33, sustentou que "O Estado português tem, pois, o poder de conciliar o acesso do público a documentos oficiais com o direito à proteção de dados pessoais, mas somente *nos termos do* [Regulamento Geral sobre a Proteção de Dados]". A referida Comissão considera que o regime é necessariamente sempre o do Regulamento Geral sobre a Proteção de Dados, podendo o legislador nacional, em alternativa, incumbir a Comissão de Acesso aos Documentos Administrativos de o fazer *ou* atribuir essa competência a si própria.

[21] Cfr. artigo 26.º, n.º 1, da Constituição. Sobre o direito à privacidade no ordenamento jurídico português, cfr., entre outros, A. Menezes Cordeiro, *Tratado de direito civil*, IV[5], Coimbra: Almedina, 2019, pp. 270-282; A. Sousa Pinheiro, Privacy *e protecção de dados*, *per totum*; R. Medeiros / A. Cortês, *sub* artigo 26.º, in J. Miranda / R. Medeiros, *Constituição portuguesa anotada*, I[2], Coimbra: Coimbra Editora, 2010, pp. 619-626; J. J. Gomes Canotilho / V.

como se sabe, que só a lei os pode restringir e apenas para tutelar outros direitos ou bens constitucionais, respeitando, designadamente, o princípio da proporcionalidade[24]. Entre esses outros direitos e bens constitucionais, conta-se o direito de acesso à informação administrativa[25];

(ii) Da mesma forma, tanto o direito regional europeu dos direitos humanos (do Conselho da Europa)[26] quanto o direito (primário) da União Europeia[27] protegem tanto o direito à proteção de dados pessoais quanto o direito de acesso aos documentos administrativos – sem que seja dada prevalência apriorística a qualquer um deles (como, aliás, não podia deixar de ser[28]);

MOREIRA, *Constituição da República Portuguesa anotada*, I[4], Coimbra: Coimbra Editora, 2007, pp. 461-474; D. DUARTE, *A norma de legalidade procedimental administrativa*, pp. 831-839; J. DE OLIVEIRA ASCENSÃO, 'A reserva da intimidade da vida privada e familiar', Revista da Faculdade de Direito da Universidade de Lisboa, XLIII/1, 2002, pp. 9-25; P. MOTA PINTO, 'A proteção da vida privada na jurisprudência do Tribunal Constitucional', Jurisprudência Constitucional, n.º 10, 2006, pp. 13-28; ID., 'A limitação voluntária do direito à reserva sobre a intimidade da vida privada', in J. DE FIGUEIREDO DIAS *et al.* (eds.), *Estudos em homenagem a Cunha Rodrigues*, II, Coimbra: Coimbra Editora, 2001, pp. 527-558; ID., 'A proteção da vida privada e a Constituição', Boletim da Faculdade de Direito da Universidade de Coimbra, n.º 76, 2000, pp. 153-204; ID., 'O direito à reserva sobre a intimidade da vida privada', Boletim da Faculdade de Direito da Universidade de Coimbra, LXIX, 1993, pp. 479-586; R. CAPELO DE SOUSA, *O direito geral de personalidade*, Coimbra: Coimbra Editora, 1995, pp. 316-351; R. AMARAL CABRAL, 'O direito à intimidade da vida privada: breve reflexão acerca do artigo 80.º do Código Civil', in AA.VV., *Estudos em memória do Professor Paulo Cunha*, Lisboa: s.n., 1988, pp. 373-406.

[22] Cfr. artigo 35.º da Constituição. Especificamente sobre o direito à proteção de dados pessoais cfr., entre outros, F. URBANO CALVÃO, 'O direito fundamental à proteção dos dados pessoais e a privacidade 40 anos depois', in M. A. VAZ *et al.* (coord.), Jornadas *nos 40 anos da Constituição da República Portuguesa. Impacto e evolução*, Porto: Universidade Católica Editora, 2017, pp. 85-101; C. SARMENTO E CASTRO, '40 anos de «utilização da informática» – o artigo 35.º da Constituição da República Portuguesa', e-Pública, vol. III, n.º 3, 2016, pp. 43-66; J. DE SEABRA LOPES, 'O artigo 35.º da Constituição: da génese à atualidade e ao futuro previsível', Fórum de Proteção de Dados, n.º 2, 2016, pp. 14-51; A. SOUSA PINHEIRO, Privacy *e protecção de dados*, *per totum*; M. P. RIBEIRO DE FARIA, *sub* artigo 35.º, in J. MIRANDA / R. MEDEIROS, *Constituição*, I[2], pp. 779-801; J. J. GOMES CANOTILHO / V. MOREIRA, *Constituição*, I[4], pp. 547-558.

[23] O princípio da proteção de dados constitui também, desde 2015, um princípio geral da atividade administrativa, plasmado no artigo 18.º do Código do Procedimento Administrativo. C. J. FAUSTO DE QUADROS, *sub* artigo 18.º, in AA.VV., *Comentário à revisão do Código do Procedimento Administrativo*, Coimbra: Almedina, 2016, p. 47, considera que "esta matéria tinha que ser disciplinada num Código do Procedimento Administrativo"; no mesmo sentido, cfr. A. SOUSA PINHEIRO, 'A proteção de dados no novo Código do Procedimento Administrativo', in C. AMADO GOMES *et al.* (coord.), *Comentários ao novo Código do Procedimento Administrativo*[2], pp. 253, 275, 278. Não obstante, tem-se – tal como F. PAES MARQUES, 'Acesso à informação administrativa', pp. 263-264 – dificuldade em aderir a essa posição.

[24] Cfr. artigo 18.º, n.º 2, da Constituição.

[25] Cfr. artigos 48.º, n.º 2, e 268.º, n.[os] 1 e 2, da Constituição.

[26] Cfr., designadamente, Convenção do Conselho da Europa n.º 205 sobre o Acesso a Documentos Oficiais, assinada em Tromsø a 18 de junho de 2009, e Convenção do Conselho da Europa n.º 108 para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, assinada em Estrasburgo a 28 de janeiro de 1981, modificada pelo Protocolo que altera a Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, assinado em Estrasburgo a 10 de janeiro de 2018. Para uma panorâmica, cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS / COUNCIL OF EUROPE, *Handbook on European data protection law*, Luxemburgo: Publications Office of the EU, 2018, pp. 17-35; A. PETERS, 'Towards transparency as a global norm', pp. 534-607.

[27] Cfr., quanto à proteção de dados, artigo 8.º da Carta dos Direitos Fundamentais da União Europeia – sobre ele, com referências, cfr. T. LOCK, *sub* artigo 8.º, in M. KELLERBAUER / M. KLAMERT / J. TOMKIN (eds.), *Commentary on the EU Treaties and the Charter of Fundamental Rights*, Oxford: Oxford University Press, 2019, pp. 2121-2127; H. KRANENBORG, *sub* artigo 8.º, in S. PEERS *et al.* (eds.), *The EU Charter of Fundamental Rights: a commentary*, Oxford: Hart, 2014, pp. 223-266; C. SARMENTO E CASTRO, *sub* artigo 8.º, in A. SILVEIRA / M. CANOTILHO (coord.), *Carta dos Direitos Fundamentais da União Europeia comentada*, Coimbra: Almedina, 2013, pp. 120-128. E quanto ao acesso aos documentos administrativos, cfr. artigo 42.º da Carta dos Direitos Fundamentais da União Europeia – sobre ele, cfr. P. CRAIG, *EU administrative law*[3], Oxford: Oxford University Press, 2019, pp. 388-400; T. LOCK, *sub* artigo 42.º, in in M. KELLERBAUER / M. KLAMERT / J. TOMKIN (eds.), *Commentary*, p. 2208; D. CURTIN / J. MENDES, *sub* artigo 42.º, in in S. PEERS *et al.* (eds.), *The EU Charter*, pp. 1099-1120; C. GOUVEIA ALVES, *sub* artigo 42.º, in A. SILVEIRA / M. CANOTILHO (coord.), *Carta dos Direitos Fundamentais*, pp. 490-498.

[28] Sobre a inadequação e a indesejabilidade de uma hierarquização material fechada entre direitos fundamentais, cfr. J. DE MELO ALEXANDRINO, *A estruturação do sistema de direitos, liberdades e garantias*, II, pp. 398-414.

(iii) O próprio Regulamento Geral sobre a Proteção de Dados determina que "os dados pessoais que constem de documentos oficiais na posse de uma autoridade pública ou de um organismo público ou privado para a prossecução de atribuições de interesse público podem ser divulgados pela autoridade ou organismo nos termos do direito da União ou do Estado-Membro que for aplicável à autoridade ou organismo público, a fim de conciliar o acesso do público a documentos oficiais com o direito à proteção dos dados pessoais nos termos do presente regulamento"[29] – isto é, assume que ambos os direitos em causa devem ser harmonizados, admitindo que o acesso a documentos administrativos que contenham dados pessoais possa beneficiar de um regime material próprio;

(iv) A nível nacional, a Lei de Execução do Regulamento Geral sobre a Proteção de Dados trilhou esse caminho, tendo determinado que "O acesso a documentos administrativos que contenham dados pessoais rege-se pelo disposto na [Lei de Acesso aos Documentos Administrativos]"[30].

8. Quanto ao regime material concreto que lhe é aplicável, entende-se que é o que resulta da Lei de Acesso aos Documentos Administrativos – que é, em alguns aspetos, efetivamente menos protetor para o titular dos dados do que o que resulta do Regulamento Geral sobre a Proteção de Dados. Por outras palavras: dessa opção legislativa resulta uma redução do âmbito de proteção do fundamental à proteção dos dados pessoais.

Mas essa afetação desvantajosa do conteúdo do direito em causa consta de um ato legislativo e é resultado da ponderação de outros bens constitucionais igualmente relevantes: a transparência administrativa enquanto valor objetivo e o direito constitucional de acesso à informação enquanto direito fundamental. Ambos os direitos estão, "por conseguinte, sujeitos à ponderação casuística e sequencial com outros direitos de acordo com um critério de proporcionalidade, tendo em conta os valores em jogo" em cada situação da vida em que a questão se coloque através de uma operação de concordância prática[31]. Como referiu o próprio Tribunal Constitucional, "a proibição contida no artigo 35.º, n.º 4, da [Constituição], como o próprio preceito indica, não é absoluta, admitindo excepções que poderão ser definidas pelo legislador ordinário"[32]. Não se considera, por isso, ser possível uma ponderação apriorística, como a propugnada pela Comissão Nacional de Proteção de Dados, para quem a redução da proteção dos direitos dos titulares de dados pessoais em posse da administração só pode "ter lugar por razões que se prendem com o exercício específico da atividade pública e não simplesmente pelo facto de os dados pessoais estarem na posse de entidades públicas"[33].

[29] Cfr. artigo 86.º do Regulamento Geral sobre a Proteção de Dados. Sobre ele, cfr. H. KRANENBORG, *sub* artigo 86.º, in C. KUNER *et al.* (eds.), *The EU General Data Protection Regulation: a commentary*, Oxford: Oxford University Press, 2020, pp. 1213-1223.

[30] Cfr. artigo 26.º da Lei n.º 58/2019, de 8 de agosto.

[31] Na expressão usada no Parecer da Comissão de Acesso aos Documentos Administrativos n.º 132/2014. No mesmo sentido, cfr. F. PAES MARQUES, 'Acesso à informação administrativa', pp. 264-267.

[32] Cfr. Acórdão do Tribunal Constitucional n.º 213/2008.

[33] Cfr. Parecer da Comissão Nacional de Proteção de Dados n.º 20/2018, p. 33v. Por sua vez, no seu Parecer n.º 11/2016, p. 8, faz-se uma redução teleológica do alcance do princípio da transparência administrativa: "o princípio da administração aberta […] não impõe nem fundamenta, por si só, a abertura de todos os documentos administrativos com dados pessoais à consulta ou mesmo à curiosidade de terceiros. A [sua] *ratio* […] é a de assegurar um controlo pelos cidadãos das decisões políticas e administrativas […] e […] a de garantir a participação democrática dos cidadãos nos processos decisórios. Mas, para o efeito, não precisam, por regra, de conhecer a informação individualizada ou individualizável; na generalidade das situações, será suficiente o conhecimento dos dados anonimizados. Para essa finalidade, o acesso a dados pessoais tem de estar diretamente relacionado com a

9. Em qualquer caso, os riscos de interpretações divergentes entre um e outro regimes são bastante menores desde a Lei de Acesso aos Documentos Administrativos de 2016. De facto, se, em matéria de acesso à informação administrativa, a proteção da privacidade e dos dados pessoais desde sempre foi materializada no conceito de *documento nominativo*, com a aprovação desse ato legislativo passou a abdicar-se de uma definição própria e autónoma do conceito. Passou, ao invés, a operar um reenvio recetício, definindo-o como o "documento administrativo que contenha dados pessoais, definidos nos termos do regime legal de proteção de dados pessoais"[34]. Verifica-se o mesmo, de resto, para o acesso à informação procedimental, visto que o Código do Procedimento Administrativo determina que o acesso é feito "sem prejuízo da proteção dos dados pessoais nos termos da lei"[35].
Ora, esse regime legal para que uma e outra normas remetem é, hoje, como se sabe, o que consta do Regulamento Geral sobre Proteção de Dados, que define dados pessoais como:

> "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); 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"[36].

Sendo que o respetivo tratamento consiste:

> "[n]uma operação ou [n]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"[37].

De onde se retira que – *no vocabulário do direito do acesso à informação administrativa* – qualquer acesso a um *documento nominativo* corresponde – *no léxico do direito da proteção*

---

participação ativa e determinante do titular dos dados naqueles processos decisórios, por só assim estar em causa o controlo e participação públicos por parte dos cidadãos".

[34] Cfr. artigo 3.º, n.º 1, alínea *b)*, da Lei de Acesso aos Documentos Administrativos. O Código do Procedimento Administrativo não dispõe de uma definição autónoma. Sobre o conceito de 'documento nominativo' à luz do regime anterior, cfr. A. SOUSA PINHEIRO, Privacy *e protecção de dados*, pp. 887-893; A. BRANDÃO DA VEIGA, *Acesso à informação*, pp. 127-133; S. PRATAS, *Lei do acesso e da reutilização dos documentos administrativos*, Lisboa: Dislivro, 2008, pp. 61-72; J. R. GONÇALVES, *Acesso à informação das entidades públicas*, Coimbra: Almedina, 2002, pp. 61-128. Para uma análise cronológica, cfr. L. NETO, 'Right of access to public information: the Portuguese case', in H.-J. BLANKE / R. PERLINGEIRO (eds.), *The right of access to public information: an international comparative legal survey*, Berlim: Springer, 2018, pp. 375-381.

[35] Cfr. artigo 83.º, n.º 2, do Código do Procedimento Administrativo.

[36] Cfr. artigo 4.º, n.º 1, do Regulamento Geral sobre a Proteção de Dados. Sobre o conceito, cfr. GRUPO DE TRABALHO DO ARTIGO 29.º, 'Parecer n.º 04/2007 sobre o conceito de dados pessoais', de 20 de junho de 2007, 01248/07/PT WP 136, disponível em URL: https://bit.ly/2Q9UprC; na doutrina, cfr. L. A. BYGRAVE / L. TOSONI, *sub* artigo 4.º, n.º 1, in C. KUNER *et al.* (eds.), *The EU General Data Protection Regulation*, pp. 103-116; A. BARRETO MENEZES CORDEIRO, *Direito da proteção de dados*, Coimbra: Almedina, 2020, pp. 107-142; ID., 'Dados pessoais: conceito, extensão e limites', Revista de Direito Civil, ano 3, n.º 2, 2018, pp. 297-321.

[37] Cfr. artigo 4.º, n.º 2, do Regulamento Geral sobre a Proteção de Dados. Sobre ele, na doutrina, cfr. L. TOSONI / L. A. BYGRAVE, *sub* artigo 4.º, n.º 2, in C. KUNER *et al.* (eds.), *The EU General Data Protection Regulation*, pp. 116-123; entre nós, cfr. A. BARRETO MENEZES CORDEIRO, *Direito da proteção de dados*, pp. 143-166.

de dados – a várias operações de tratamento de dados pessoais levadas a cabo pelo responsável pelo tratamento: pressupõe que a administração pública (responsável pelo tratamento) recolhe e conserva esses dados e que depois permite, ou não, a sua consulta a um terceiro.

Tendo a Lei de Acesso aos Documentos Administrativos passado a especificar que todos os pedidos de acesso a documentos administrativos que não fossem relativos a 'dados sensíveis' – salvaguardando assim o regime aplicável a estes últimos – seguiriam o regime aí previsto, ao ter determinado que:

> "nos pedidos de acesso a documentos nominativos que não contenham dados pessoais 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"[38].

10. Da articulação de regimes relativos ao acesso de terceiros a informação administrativa não procedimental que contenham dados pessoais e ao acesso de terceiros a informação administrativa procedimental que também incluam dados pessoais sobressai um aspeto potencialmente problemático[39]. É que, se a Lei de Acesso aos Documentos Administrativos tem um regime próprio, o mesmo não sucede com o Código do Procedimento Administrativo, que remete em bloco para o Regulamento Geral sobre a Proteção de Dados.

Daqui resulta que um terceiro pode, ao abrigo do princípio do arquivo aberto, exercer o direito de acesso a *documentos nominativos* detidos pela administração mediante o preenchimento de uma de duas condições alternativas:

> "a) Se estiver munido de autorização escrita do titular dos dados que seja explícita e específica quanto à sua finalidade e quanto ao tipo de dados a que quer aceder;
> b) Se demonstrar fundamentadamente ser titular de um interesse direto, pessoal, legítimo e constitucionalmente protegido suficientemente relevante, após ponderação, no quadro do princípio da proporcionalidade, de todos os direitos fundamentais em presença e do princípio da administração aberta, que justifique o acesso à informação"[40].
>
> Já um terceiro que pretenda ter acesso a documentos administrativos que contenham dados pessoais ao abrigo ao direito de acesso à informação administrativa procedimental apenas o pode fazer quando, nos termos do Regulamento Geral sobre a Proteção de Dados,
>
> "O tratamento [seja] necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os

[38] Cfr. artigo 6.º, n.º 9, da Lei de Acesso aos Documentos Administrativos. Sobre dados sensíveis, cfr. artigos 9.º e 4.º, n.os 13 a 15, do Regulamento Geral sobre a Proteção de Dados. Acerca dos mesmos, cfr. L. A. BYGRAVE / L. TOSONI, *sub* artigo 4.º, n.os 13, 14 e 15, in C. KUNER *et al.* (eds.), *The EU General Data Protection Regulation*, pp. 196-225; L. GEORGIEVA / C. KUNER, *sub* artigo 9.º, in C. KUNER *et al.* (eds.), *The EU General Data Protection Regulation*, pp. 365-385; na doutrina nacional, A. BARRETO MENEZES CORDEIRO, *Direito da proteção de dados*, pp. 132-142.
[39] Secunda-se aqui F. PAES MARQUES, 'Acesso à informação administrativa', pp. 264-267.
[40] Cfr. artigo 6.º, n.º 5, da Lei de Acesso aos Documentos Administrativos.

> interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança"[41].

Assim, enquanto a Lei de Acesso aos Documentos Administrativos se refere à titularidade de um "interesse direto, pessoal, legítimo e constitucionalmente protegido suficientemente relevante", o Regulamento Geral sobre a Proteção de Dados – e, portanto, o Código do Procedimento Administrativo – utiliza a referência a "interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros".
Esta disparidade levanta duas ordens de questões:

> (i) Uma respeitante à natureza do interesse necessário para que seja satisfeita a pretensão do terceiro de acesso à informação;
> (ii) Outra atinente à distribuição do ónus da prova.

Quanto à primeira (i), entende-se que, apesar da diferente formulação linguística com que se apresentam *prima facie* ao intérprete, se devem considerar equivalentes. Assim, como resulta do sistema de direitos fundamentais português, apenas direitos constitucionalmente protegidos podem fundamentar uma intervenção restritiva sobre os direitos fundamentais à privacidade e à proteção de dados[42]. Pelo que um mero interesse, de facto ou de direito, de um terceiro, ainda que justificado, dificilmente logrará prevalecer, em concreto, sobre os direitos fundamentais à privacidade e à proteção dos seus dados pessoais[43]. Nesse caso, note-se que é a própria Lei de Acesso aos Documentos Administrativos que exige que o requerente que, nesse caso, especifique a finalidade do acesso, ao determinar que:

> "Os documentos nominativos comunicados a terceiros não podem ser utilizados ou reproduzidos de forma incompatível com a autorização concedida, com o fundamento do acesso, com a finalidade determinante da recolha ou com o instrumento de legalização, sob pena de responsabilidade por perdas e danos e responsabilidade criminal, nos termos legais"[44].

De resto, é o que tem feito – e bem – a própria Comissão de Acesso aos Documentos Administrativos, impondo uma análise da pretensão do particular em dois passos, averiguando:

---

[41] Cfr. artigo 6.º, n.º 1, alínea *f)*, do Regulamento Geral sobre a Proteção de Dados, aplicável *ex vi* artigo 83.º, n.º 2, do Código do Procedimento Administrativo. Para a interpretação da referida alínea daquele regulamento, cfr. GRUPO DE TRABALHO DO ARTIGO 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, *máxime* pp. 36-76, disponível em URL: https://bit.ly/3iUypNG. Na doutrina, cfr. W. KOTSCHY, *sub* artigo 6.º, in C. KUNER *et al.* (eds.), *The EU General Data Protection Regulation*, pp. 321-345; A. BARRETO MENEZES CORDEIRO, *Direito da proteção de dados*, pp. 223-237; ID., 'O tratamento de dados pessoais fundado em interesses legítimos', Revista de Direito e Tecnologia, 2019, pp. 1-32.
[42] Segue-se aqui F. PAES MARQUES, 'Acesso à informação administrativa', pp. 266-267. No mesmo sentido, cfr. A. SOUSA PINHEIRO, 'A proteção de dados', pp. 259, 275.
[43] Cfr., já antes, T. FIDALGO DE FREITAS, 'Administrative transparency in Portugal', p. 681; A. SOUSA PINHEIRO, Privacy *e protecção de dados*, p. 890. Para uma aplicação, cfr. J. CAUPERS, 'Acesso a documentos nominativos: direito à informação ou reserva da intimidade?', Cadernos de Justiça Administrativa, n.º 1, 1997, pp. 33-34.
[44] Cfr. artigo 8.º, n.º 2, da Lei de Acesso aos Documentos da Administração.

(1) se o motivo eventualmente invocado para o acesso é (ou não) suficiente para o facultar; e (2) se, da efetivação do direito de acesso, não resulta lesão para os interesses do titular da informação[45].

No que toca à segunda questão (ii), considera-se que o ónus da prova de que não existe qualquer violação de dados pessoais impende sobre o requerente – e não sobre a administração que detém o documento, em resposta ao pedido do terceiro[46]. Por outras palavras: perante pretensões de terceiros de acesso a *documentos* (administrativos) *nominativos*, a regra deve ser a de que a privacidade e a proteção de dados pessoais são salvaguardadas, salvo razões preponderantes em contrário e na medida em que estas existam[47].

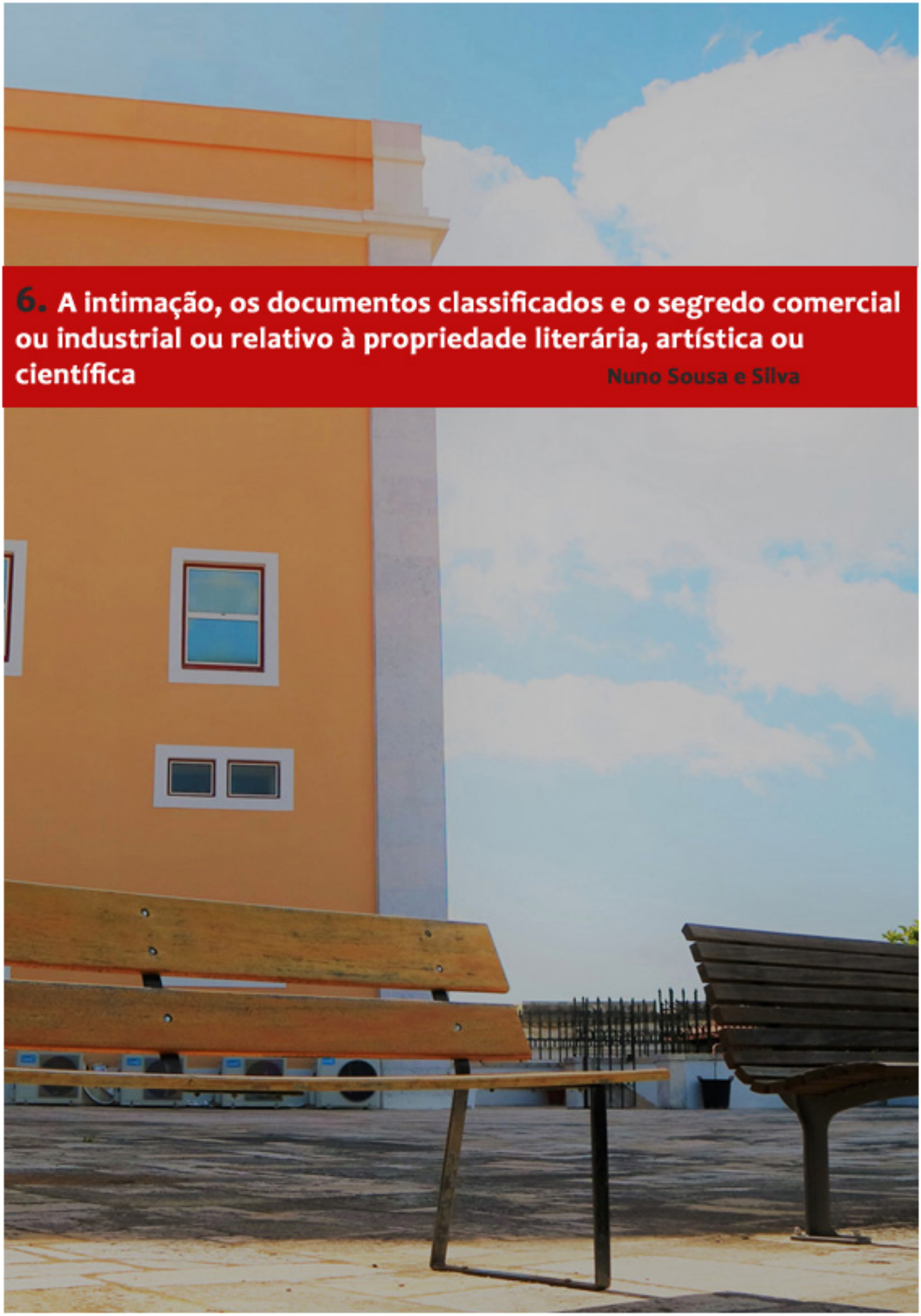
[45] Cfr. Parecer da Comissão de Acesso aos Documentos Administrativos n.º 73/2017.

[46] Como resulta do artigo 35.º, n.º 4, da Constituição. Neste sentido, cfr. Parecer da Comissão de Acesso aos Documentos Administrativos n.º 59/2003. Já assim se defendia, na vigência da Lei de Acesso aos Documentos Administrativos de 2007, em T. FIDALGO DE FREITAS, 'Administrative transparency in Portugal', p. 681; em sentido concordante, entretanto, cfr. F. PAES MARQUES, 'Acesso à informação administrativa', p. 267, com referência (discordante) ao Acórdão do Supremo Tribunal Administrativo de 20 de dezembro de 2017, Proc. n.º 0870/17, que sustentou que "do artigo 83.º do CPA não resulta a existência de qualquer ónus de invocar nada relativamente aos terceiros abrangidos nos documentos em causa, antes será a Administração que terá de invocar que os mesmos violam a proteção dos dados pessoais nos termos da lei".

[47] Como exemplo de uma decisão bem fundamentada, cfr. Acórdão do Tribunal Central Administrativo – Sul de 22 de janeiro de 2009, Proc. n.º 04527/08, em que um particular solicitou a um município a lista de todos os processos de contraordenação por infrações urbanísticas de 2006 a 2008, especificando o valor das multas aplicadas e os nomes dos réus. O Tribunal considerou que, sem a autorização destes últimos, a mera indicação, no requerimento em causa, de que tais elementos estavam destinados a "fins judiciais" não seria bastante para demonstrar a existência de um interesse suficientemente relevante de acordo com o princípio da proporcionalidade. No mesmo sentido, no âmbito do direito da União Europeia e a propósito de questão similar, cfr. o Acórdão do Tribunal de Justiça da União Europeia de 16 de julho de 2015, *ClientEarth c. EFSA*, C-615/13 P, EU:C:2015:489, parágrafo 47: "cabe primeiro a quem requer essa transferência demonstrar a sua necessidade. Se for feita essa demonstração, cabe então à instituição em causa verificar se não existem motivos para supor que os interesses legítimos da pessoa em causa podem ser prejudicados por essa transferência".

Vídeo da apresentação

https://educast.fccn.pt/vod/clips/2p6tj7fik9/ipod.m4v?locale=pt



6. A intimação, os documentos classificados e o segredo comercial ou industrial ou relativo à propriedade literária, artística ou científica

Nuno Sousa e Silva

CENTRO
DE ESTUDOS
JUDICIÁRIOS

6. A INTIMAÇÃO, OS DOCUMENTOS CLASSIFICADOS E O SEGREDO COMERCIAL OU INDUSTRIAL OU RELATIVO À PROPRIEDADE LITERÁRIA, ARTÍSTICA OU CIENTÍFICA*

Nuno Sousa e Silva**

Bibliografia

– ALEXANDRE BRANDÃO DA VEIGA, *Acesso à Informação da Administração Pública pelos Particulares* (Almedina 2007)
– CARLA AMADO GOMES / ANA F. NEVES / PEDRO LOMBA (coord.), *Os Segredos no Direito* (AAFDL 2019)
– DÁRIO MOURA VICENTE, 'Segredo Comercial e Acesso à Informação Administrativa' in AAVV, *Estudos em Homenagem ao Prof. Doutor Sérvulo Correia*, vol. III (Coimbra Ed. 2010) pp. 289-297
– JOSÉ RENATO GONÇALVES, *Acesso à Informação das Entidades Públicas* (Almedina 2002)
– NUNO SOUSA E SILVA, 'What exactly is a trade secret under the proposed directive?' in Journal of Intellectual Property Law and Practice [2014] pp. 923-932
– NUNO SOUSA E SILVA, 'O Segredo de Negócio como Escudo e como Espada' in MARIA FERNANDA PALMA / AUGUSTO SILVA DIAS / PAULO DE SOUSA MENDES (eds), *Estudos sobre Law Enforcement, Compliance e Direito Penal* (Almedina 2018) pp. 209-263
– NUNO SOUSA E SILVA, 'A nova disciplina dos segredos de negócio: análise e sugestões' in Revista de Direito Intelectual 1/2019 pp. 49-81
– RAQUEL CARVALHO, *O Direito à Informação Administrativa Procedimental* (UCE 1999)
– SARA YOUNIS AUGUSTO DE MATOS, 'Intimação para a prestação de informações, consulta de processos ou passagem de certidões: entre o que se fez e o que ficou por fazer' in CARLA AMADO GOMES / ANA F. NEVES / TIAGO SERRÃO (coord.), *Comentários à Revisão do ETAF e do CPTA* (AAFDL 2017) pp. 917-937
– SÉRGIO PRATAS, *A (nova) Lei de Acesso aos Documentos Administrativos* (Almedina 2018)

* Apresentação decorrente da ação de formação contínua do CEJ "A tutela urgente no contencioso administrativo", realizada a 12 e 13 de dezembro de 2019.
** Professor na Faculdade de Direito da Universidade Católica Portuguesa, Porto.

Vídeo da apresentação

https://educast.fccn.pt/vod/clips/anzel14sf/ipod.m4v?locale=pt

Título:
Direito à InformaçãoAdministrativa
e Proteçãode Dados Pessoais

Ano de Publicação: 2021

ISBN: 978-989-9018-82-2

Série: Formação Contínua

Edição: Centro de Estudos Judiciários

Largo do Limoeiro

1149-048 Lisboa

cej@mail.cej.mj.pt