Privacidade e Proteção de Dados do Município de Lisboa

LISBOA

Privacidade e Proteção de Dados do Município de Lisboa

Imagem | Adobe Stock | de Iren Moroz

ÍNDICE

1 | PREFÁCIO

Aceitei com muito agrado o convite da Professora Doutora Cristina Caldeira, Encarregada de Proteção de Dados da Câmara Municipal de Lisboa, para escrever o prefácio de *Privacidade e Proteção de Dados Pessoais do Município de Lisboa,* uma obra de grande atualidade e relevância científica e prática.

O tratamento de dados pessoais é uma matéria que exige um constante acompanhamento, sensibilização e formação. São inúmeros os deveres específicos que resultam do Regulamento Geral sobre a Proteção de Dados e respetiva legislação nacional de execução, bem como os riscos e impactos acrescidos a que as instituições, sujeitas a esta regulação, têm continuamente de gerir e mitigar na aplicação deste Direito.

Na Câmara Municipal de Lisboa, a proteção de dados pessoais tem sido um vetor essencial de ação e tem contado, na sua implementação e execução, com uma grande colaboração de departamentos de todas as áreas municipais. Um exemplo eloquente deste esforço de aprimoramento foi a realização de duas auditorias, uma interna e outra externa, de avaliação da conformidade do Município de Lisboa com o Regulamento Geral sobre a Proteção de Dados. Também a necessidade de sensibilizar decisores, serviços e trabalhadores para a adoção de medidas técnicas de aprofundamento do grau de conformidade com a legislação em vigor tem motivado a Encarregada de Proteção de Dados da Câmara Municipal de Lisboa para a implementação de mecanismos de difusão do conhecimento nesta matéria.

Privacidade e Proteção de Dados do Município de Lisboa tem por tema principal a proteção de dados pessoais, sem prejuízo do desenvolvimento de matérias que, paralelamente, desempenham um papel fulcral na abordagem seguida nesta sede: a privacidade, a cibersegurança, e a tutela dos direitos fundamentais. Organizada em artigos temáticos, da autoria de académicos de reconhecido mérito na área da proteção de dados, esta coletânea de textos seletos apresenta múltiplas visões sobre os temas estruturantes da proteção de dados, com particular enfoque na realidade e especificidades das autarquias locais.

As páginas que se seguem assentam na certeza de que o futuro que vamos construindo diariamente no Município de Lisboa depende, em muito boa medida, do contínuo esclarecimento da consciência individual e coletiva sobre as responsabilidades associadas ao tratamento de dados pessoais. A leitura atenta e cuidada de cada um dos artigos de *Privacidade e Proteção de Dados Pessoais do Município de Lisboa* é mais um passo nesse movimento de crescente consciencialização e responsabilização.

O Vice-Presidente da Câmara Municipal de Lisboa,

Filipe Anacoreta Correia

Enquadramento da Obra

O Município de Lisboa não é alheio à mudança de paradigma a que se assiste na Era Digital, com implicações estruturais no funcionamento da instituição, levando a uma adequação exigente e cuidada dos seus processos de tratamento de dados pessoais, tendo em vista a garantia dos direitos e liberdades dos munícipes, e dos titulares dos dados em geral.

Para assinalar as celebrações do Dia da Proteção de Dados (28 de janeiro), o Município de Lisboa dirigiu um convite a um grupo de doutrinadores, professores e investigadores de reconhecido mérito, nos domínios da privacidade e proteção de dados, que generosamente responderam ao convite, disponibilizando o seu saber e a sua experiência.

O resultado é uma obra de natureza teórico-prática, uma referência nos domínios da privacidade, proteção de dados, inteligência artificial e governação de dados, que nos ajudará a trilhar os desafios que o cumprimento das normas de proteção de dados nos coloca.

O artigo de abertura é da autoria do Professor Doutor António Barreto Menezes Cordeiro, uma resenha histórica do Direito da Proteção de Dados, desde os anos 60 do século XX até à contemporaneidade, na qual são elencados os principais conceitos e princípios que dão corpo a este ramo jurídico, autónomo, específico e eclético. Numa perspetiva histórica, salienta que embora o nascimento do Direito da proteção de dados tenha ocorrido nas fronteiras do Direito público, esta hegemonia foi quebrada, sendo a legislação na área da proteção de dados, aplicada, quer ao tratamento de dados produzidos por sujeitos de Direito público, quer por sujeitos de Direito privado.

O Professor Doutor Alexandre L. Dias Pereira, reflete sobre a proteção de dados pessoais a partir do Regulamento Geral de Proteção de Dados (*RGPD*), na perspetiva do responsável pelo tratamento, realçando as suas novas obrigações e, em especial o papel central do responsável pelo tratamento no regime jurídico dos dados das pessoas humanas. Conclui pela especial relevância da proteção dos dados pessoais e da Inteligência Artificial.

A segurança no tratamento dos dados aplicada ao poder local foi defendida pelo Professor Manuel David Masseno, responsabilidade que o *RGPD* imputa, quer ao responsável pelo tratamento, quer ao subcontratante, e que está diretamente relacionada com o cumprimento dos princípios da integridade e confidencialidade. O risco associado à utilização das novas tecnologias para os direitos e liberdades das pessoas singulares, constitui uma matéria central amplamente tratada, com níveis de risco diferenciados atendendo à natureza, âmbito, contexto e finalidades do tratamento dos dados, exigindo que o responsável pelo tratamento proceda, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. A severidade e probabilidade do risco chama à colação as medidas técnicas e organizativas de proteção dos dados pessoais, nomeadamente a pseudonomização e anonimização, que são aplicáveis pelo poder local.

Tendo em conta a crescente tendência de publicação de conteúdos nas redes sociais pela Administração Local, a Equipa de Projeto de Proteção de Dados Pessoais do Município de Lisboa, em autoria coletiva: Jorge Gomes da Silva, Maria de Medeiros, Maria Helena Silva e Telma Vitória, procura demonstrar as principais consequências da publicação de fotografias e vídeos nestas plataformas, fornecendo, ao mesmo tempo, a partilha de boas práticas que contribuem para a melhoria da conformidade com o *RGPD*.

A Professora Doutora Isabel Celeste M. Fonseca e o Investigador Joel A. Alves, analisam a Orientação da CNPD de 1 de abril de 2023, sobre a publicação na *Internet* das atas de reuniões de órgãos colegiais autárquicos e as respetivas consequências práticas.

O Professor Doutor Francisco Rodrigues Rocha aborda a temática da conservação dos dados pessoais e a dificuldade da aplicação prática dos prazos de conservação, tendo em conta a sua determinação prévia e abstrata.

A conservação dos metadados é aprofundadamente tratada pelo Professor Doutor Duarte Rodrigues Nunes, fazendo alusão às implicações do Acórdão do Tribunal Constitucional n.º 268/2022, que reformulou a Lei n.º 32/2008, de 17 de julho, e em concreto, a questão sobre a admissibilidade (ou não), da obtenção e valoração de metadados, conservados pelos respetivos operadores, bem como das provas obtidas através destes.

O Professor Doutor Pedro Rebelo Botelho Alfaro Velez apresenta-nos, no seu texto, as visões contemporâneas dos direitos fundamentais, procurando traçar o panorama das diversas culturas de direitos, bem como das contraculturas alternativas nas atuais democracias ocidentais, com destaque para o quadro europeu, ainda que abrangendo o cenário norte-americano.

A partir de fontes normativas europeias e nacionais, o Professor Doutor Alexandre Sousa Pinheiro aborda a governação e a reutilização de dados, bem como a proteção de dados pessoais. Baseando-se na Estratégia de Dados da União Europeia, analisa a evolução do mercado de dados europeu, dando nota dos serviços de intermediação de dados. Analisa também, a conciliação do *RGPD* com as diversas formas de extrair informação.

Por último, o risco, mas também os resultados promissores da aplicação das novas tecnologias, em especial da Inteligência Artificial no setor da saúde, é o tema abordado pela Professora Doutora Cristina Maria de Gouveia Caldeira. A vulnerabilidade da pessoa humana, designadamente na doença, é igualmente uma temática analisada, não só no plano legal, mas também no plano da bioética. As circunstâncias que ditam a sua fragilidade, permitem-lhe também o gozo de um regime reforçado de proteção no âmbito do Direito Europeu.

Os contributos reunidos na obra "Privacidade e Proteção de Dados Pessoais do Município de Lisboa", promovem uma reflexão, conduzida pela mão de especialistas, sobre os desafios da Era Digital.

Neste exercício, a Administração Autárquica, na sua relação de estreita proximidade, interventiva e propedêutica e em conexão com munícipes e entidades locais de diversa natureza jurídica, é um dos principais agentes da mudança, através do incentivo a uma alteração de mentalidades e, consequentemente de procedimentos, orientados no sentido da conformidade com o Direito europeu e nacional, em matéria de privacidade, proteção de dados e segurança.

A todos, dirigimos uma palavra de profunda gratidão!

Encarregada de Proteção de Dados do Município de Lisboa

Cristina M. G. Caldeira

* Professor Doutor, LLM, Faculdade de Direito da Universidade de Lisboa.

(1) Oliver Stengel/Alexander van Looy/Stephan Wallaschkowski, *Digitalzeitalter – Digitalgesellschaft: Das Ende des Industriezeitalters und Der Beginn einer neuen Epoche*, Springer VS: Wiesbaden (2017).

(2) Como ponto de partida para a matéria, veja-se: *The Palgrave Handbook of Fintech and Blockchain*, coord. Maurizio Pompella/Roman Matousek, Palgrave Macmillan: Cham (2021) e *FinTech-Handbuch: Digitalisierung, Recht, Finanzen*, 2.ª ed., Beck: Munique (2021).

(3) Decreto-Lei n.º 93/2017, de 1 de agosto.

(4) Alexandre Sousa Pinheiro, *Morada única digital*, RDA (2018), 75-77.

(5) Lei n.º 27/2021, de 17 de maio.

3 | A PREPONDERÂNCIA DO DIREITO DA PROTEÇÃO DE DADOS NA CONTEMPORANEIDADE E O SEU ENQUADRAMENTO GERAL

*A. Barreto Menezes Cordeiro**

1. A Era Digital

I. A revolução da informação iniciada, *grosso modo,* no pós-Segunda Guerra Mundial alcançou, recentemente, um estágio de consolidação e transversalidade – manifestada na sua presença nos mais variados setores económicos, sociais, políticos e culturais – que torna patente que a espécie humana vive hoje numa era distinta da iniciada com a revolução Industrial: a Era Digital(1).

Embora não seja possível afirmar em que fase da Era Digital nos encontramos – trata-se de um exercício que apenas pode ser realizado por futuros historiadores –, os dados disponíveis demonstram que estamos num ponto de não retorno, ou seja, o processo de digitalização da sociedade contemporânea é imparável. O seu eventual bloqueio ou retrocesso só é concebível num cenário de catástrofe, natural ou humana, de proporções bíblicas.

II. Numa perspetiva jurídica, a grande diferença entre a Era Digital e as eras que a antecederam reside na mudança ocorrida quanto ao local – numa aceção desmaterializada – onde o comércio jurídico ocorre: a unicidade milenar do espaço físico deu lugar, paulatinamente, a uma partilha entre o espaço físico e o espaço digital.

No âmbito do Direito privado, os avanços são particularmente evidentes no Direito do Trabalho – com a denominada 4.ª Revolução Industrial –, nos modelos de contratação emergentes – contratação eletrónica e *e-commerce* – e na incontornável FinTech(2).

No âmbito do Direito público, o impacto da Era Digital é visível nas novas formas de interação entre a Administração Pública e os particulares – recorde-se a revolucionária morada única digital(3-4) – e na adaptação dos direitos fundamentais a esta nova realidade, com Carta Portuguesa de Direitos Humanos na Era Digital(5).

2. A emergência do Direito da proteção de dados

I. A regulação específica e autónoma do tratamento de dados pessoais surge como uma resposta à utilização de mecanismos automatizados no processamento de informação pessoal. Os avanços tecnológicos (elemento objetivo) e as vantagens decorrentes dessa evolução (elemento subjetivo) impeliram tanto o sector público como o sector privado a intensificarem o tratamento de dados pessoais. As razões que motivaram o interesse destes dois sectores são distintas. No sector público, o tratamento automatizado apresentou-se como uma solução quotidiana indispensável em face do crescimento da administração pública, fruto da disseminação de agências federais[6] (EUA) ou da assunção de um modelo de Estado Social (Europa). No sector privado, o tratamento automatizado assume um papel transversal: na relação com os clientes, na gestão de *stocks*, na identificação de riscos de incumprimento, no posicionamento no mercado ou na determinação das estratégias de *marketing* e de publicidade[7].

II. Os pioneiros da década de 60 rapidamente identificaram os riscos do tratamento automatizado de dados para a privacidade do homem comum: deixa de ser possível controlar que informação é compilada a respeito de cada um de nós e de saber quem a detém a cada momento; os nossos passos, comportamentos, opiniões e atividades podem ser monitorizados em tempo real; e esta vigilância constante, com um impacto psicológico tremendo, permite ainda condicionar e manipular o nosso futuro[8].

---

[6] Vern Countryman, *The Diminishing Right of Privacy, the Personal Dossier and the Computer,* 49 Texas L Rev (1971), 837-871, 853 ss.

[7] Simitis/Hornung/Spiecker gen. Döhmann, *Introdução em Simitis/Hornung/Spiecker gen. Döhmann – Simitis/Hornung/Spiecker gen. Döhmann Datenschutzrecht, DSGVO mit BDSG,* Nomos: Baden-Baden, (2019), 6 ss; Arthur R. Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in a Information-Oriented Society,* 67 Mich L Rev (1969), 1089-1246, 1103 ss.

[8] Miller, *Personal Privacy in the Computer Age cit.*, 1107 ss; Donald N. Michael *Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy,* 33 Geo Wash L Rev (1964), 270-286, em especial 273-274.

III. As múltiplas audiências realizadas pelo *Special Subcommittee on Invasion of Privacy*[9] foram particularmente relevantes para sensibilizar não só legislador norte-americano, mas também os vários legisladores europeus que puderam aceder à vasta documentação aí produzida.

Não podemos deixar de destacar as considerações gerais tecidas, na primeira audiência de 1965, por Monroe H. Freedman, Professor de Direito[10]:

> *It is of critical importance, therefore, that modern computer technologies makes it possible to analyse, store, and retrieve quantities of data that would have been impossible to use on a comprehensive basis formerly. Thus, a central law enforcement agency can today compile dossiers of the most extensive and intensive type. The ready availability of psychological tests of tens of thousands of our citizens is therefore, not the least frightening aspect of the impact of modern technology on the relationship between the State and citizen.*

ou o nível de pormenor das preocupações manifestadas, nas audiências de 1966, por Charles A. Reich, também Professor de Direito, em relação à eventual constituição de um *National Data Center*[11]: (i) a fiabilidade da informação tende a piorar à medida que nos afastamos da fonte de recolha original; (ii) a informação recolhida para um determinado propósito pode ser erroneamente interpretada à luz de diferentes fins; ou (iii) a centralização da informação leva à sua *petrification*, ou seja, dificilmente será apagada ou sequer alterada[12].

---

(9) A. Barreto Menezes Cordeiro, *Direito da Proteção de Dados*, Almedina: Coimbra (2021), 53 ss.

(10) *Statement of Monroe H. Freedman, Associate Professor of Law, George Washington University em Special Inquiry on Invasion of Privacy (Part 1) – Hearings Before a Subcommittee of the Committee on Government Operations, House of Representatives*, 89th Congress, First Session. June 2, 3, 4, 7, 23, and September 23, 1965, U.S. Government Printing Office: Washington (1966), 348.

(11) *The Computer and Invasion of Privacy – Hearings Before a Subcommittee of the Committee on Government Operations, House of Representatives*, 89th Congress, Second Session. July 26, 27, and 28, 1966, U.S. Government Printing Office: Washington (1966), 22-35.

(12) Trata-se de uma preocupação que várias décadas volvidos motivou o reconhecimento do direito ao esquecimento.

3. A ecleticidade do Direito da Proteção de Dados

I. Numa perspetiva histórica, podemos afirmar que o Direito da proteção de dados nasceu nas fronteiras do Direito público, por duas razões principais: (i) o primeiro diploma à escala planetária a regular o Direito da Proteção de Dados – o *Hessisches Datenschutzgesetz* (HDSG), de 1970[13-14] – apenas abrangia os tratamentos de dados realizados por entidades públicas[15]; e (ii) apenas os Estados tinham, à época, meios suficientes para proceder ao tratamento de grandes quantidades de dados.

Do ponto de vista legislativo, a hegemonia do Direito Público foi rapidamente quebrada: (i) o primeiro diploma estado-unidense – o *Fair Credit Reporting Act* – data do mesmo ano (1970) e apenas regulava entidades privadas[16]; (ii) o primeiro diploma europeu com um campo de aplicação material transversal a todas as entidades e um campo de aplicação territorial nacional – o sueco *Datalag* – data de 1973[17]; e (iii) o campo de aplicação material do primeiro diploma federal alemão – o *Bundesdatenschutzgesetz* (BDSG), de 1977 – estende-se às entidades públicas e às entidades privadas[18].

II. Contemporaneamente, não vemos como não apresentar o Direito da proteção como um ramo jurídico eclético. O *RGPD* aplica-se aos tratamentos de dados produzidos por sujeitos de Direito público e por sujeitos de Direito privado. A transversalidade do *RGPD* consubstancia, de resto, um dos elementos diferenciadores do Direito europeu da proteção de dados quando confrontado com o Direito estado-unidense.

A natureza mista do Direito da proteção de dados é colocada em especial evidência no artigo 6.º[19]. Entre os vários fundamentos para o tratamento lícito de dados pessoais contam-se o consentimento dado pelo titular dos dados – tipicamente privado – e o tratamento necessário ao exercício de funções de interesse público – tipicamente público. Curiosamente, durante as negociações legislativas, vários Estados-Membros mostraram-se desfavoráveis à implementação de um Regulamento com um campo de aplicação material extensível às entidades públicas. Acabaria por vingar a posição transversal, defendida pela Comissão[20].

Numa perspetiva mais prática, é hoje evidente que a maioria dos litígios que chegam aos tribunais envolvem apenas entidades privadas. Ao contrário do que se verificava nos primórdios contemporâneos do Direito da proteção de dados, os maiores receios respeitam hoje à atuação dos grandes conglomerados privados[21].

4. A centralidade dos dados pessoais

I. O conceito de dado pessoal assume um papel nuclear na nova Era Digital, tanto do ponto de vista jurídico, como do ponto de vista económico. A expressão "os dados são o novo petróleo" (na versão original inglesa: *"data is the new oil"*[22]), cunhada a propósito das potencialidades da *Big Data,* exprime a convicção, bem enraizada, de que os dados irão representar na Era Digital um papel análogo ao desempenhado pelo petróleo e demais combustíveis fósseis a partir da Revolução Industrial.

II. A centralidade jurídica do conceito de dado pessoal advém da amplitude do seu preenchimento. Ele abarca toda a informação relativa a pessoas singulares identificadas ou identificáveis – nos termos do disposto no artigo 4.º, 1) do *RGPD*[23] – por muito insignificante ou fútil que possa parecer para o Homem comum, como bem defendeu o Tribunal Federal Constitucional alemão no início da década de 80 do século passado[24].

O conceito de informação (pessoal) extravasa, largamente, o sentido que tradicionalmente lhe é atribuído no seio dos direitos de personalidade[25]. Privacidade não é sinónimo de direitos pessoais, nem a proteção concedida pelo regime jurídico consagrado no artigo 80.º do CC é idêntica à prevista pelo Direito da proteção de dados, em todas as suas diferentes concretizações legislativas. Tanto se entende, como sendo pessoal, informação relativa à vida privada como à vida profissional e social[26].

O facto de essa informação se inscrever no contexto de uma atividade profissional não lhe pode retirar a qualificação de conjunto de dados pessoais[27].

O conceito de informação pessoal abrange, consequentemente, todos os aspetos relativos à nossa pessoa, quer sejam familiares ou sociais, privados ou públicos, físicos ou mentais.

(13) Sobre a evolução histórica do Direito alemão da proteção de dados veja-se, por todos: Spiros Simitis, *Einleitung: Geschichte – Ziele – Prinzipien em Simitis, Bundesdatenschutzgesetz,* 8.ª ed., Nomos, Baden-Baden (2014), Rn.1 ss. Em língua inglesa: Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in the Europe and the United States,* Cornell University Press: Ithaca (1992), 74 ss.

(14) Sobre a evolução histórica do Direito da proteção de dados do Estado de Hessen veja-se, para além das obras referidas na nota anterior, Spiros Simitis, *20 Jahre Datenschutz in Hessen – eine kritische Bilanz em Neunzehnter Tätigkeitsbericht des Hessischen Datenschutzbeauftragten,* 1991, 68-75.

(15) § 1 do HDSG. Esta circunscrição contribuiu para a rápida e unânime aprovação do diploma: Spiros Simitis, *Privacy – An Endless Debate,* 98 Cal L Rev (2010), 1989-2005, 1996.

(16) A. Barreto Menezes Cordeiro, *Direito* cit., 57 ss.

(17) A. Barreto Menezes Cordeiro, *Direito* cit., 64-65.

(18) A. Barreto Menezes Cordeiro, *Direito* cit., 65.

(19) As disposições legais não acompanhadas de fonte correspondem a artigos do *RGPD*.

(20) Conselho, Nota de 26-nov.–2012, 16525/12, 8 [20]: *"some delegations think this objective should not apply to the public sector, arguing from an early stage in the discussions for the need for more flexibility regarding data protection rules for the public sector, to enable them to adapt these rules to their national regimes. The Commission, on the other hand, argued that harmonisation in this area is also necessary as cross-border exchange of data is necessarily also increasing between public authorities in key areas such as taxation, social security, health, banking and financial markets supervision, and that, more generally, individuals in the European Union should be able to expect also similar levels of data protection in the public sector in Member States, given that the fundamental right to data protection did not differentiate between public and private sector"*.

(21) Johannes Masing, *Herausforderungen des Datenschutzes,* 65 NJW (2012), 2305-2311.

(22) Dennis D. Hirsch, *The Glass House Effect: Big Data, The New Oil, and the Power of Analogy,* 66 Me L Rev (2014), 374-395, 374, nota 1.

(23) Sobre o conceito de dado pessoa, veja-se, o nosso: *Dados pessoais: conceito, extensão e limites,* III RDC (2018), 297-321.

(24) BVerfG 15-dez.-1983, 37 NJW (1984), 419-428, 422. Para uma análise ao acórdão, veja-se: Spiros Simitis, *Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung,* 37 NJW (1984), 398-405 e Gerrit Hornung/Christoph Schnabel, *Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination,* 25 CLSR, (2009), 84-88.

(25) António Menezes Cordeiro, *Tratado de Direito Civil,* IV, 5.ª ed., com a colaboração de A. Barreto Menezes Cordeiro, Almedina: Coimbra (2019), 270: "Em rigor, a vida privada abrangerá tudo o que não seja público e profissional ou social".

(26) TJUE 30-mai.-2013, proc. C-342/12 *(Worten v ACT),* 18 ss; TJUE 29-jun.-2010, proc. C-28/08 *(Comissão v The Bavarian Lager),* 68 ss; TJUE 20-mai.-2003, proc. C465/00, C-138/01 e C-139/01 *(Rechnungshof v Österreichischer Rundfunk),* 64 ss, em especial 73.

(27) TJUE 16-nov.-2015, proc. C-615/13 P *(ClientEarth v PAN Europe),* 30.

A informação pode respeitar, a título meramente exemplificativo, a elementos identificativos da pessoa – nome, data de nascimento, número de cartão de cidadão ou morada – características físicas – género, altura, peso, cor dos olhos ou do cabelo – considerações íntimas – crenças, opiniões, desejos, posições políticas ou religiosas – profissionais e académicas – títulos e graus ou estatutos profissionais e laborais – ou patrimoniais – direitos de propriedade. São infindáveis as modalidades passíveis de serem concebidas.

O conceito de informação, para efeitos de aplicação do *RGPD*, abrange dados objetivos ou factuais – p. ex.: **A** nasceu em Lisboa – ou subjetivos – **A** não é um trabalhador honesto, um cliente de confiança ou um segurado cumpridor atempado das suas obrigações.

É igualmente irrelevante se os dados compilados e tratados são ou não verdadeiros. Para isso mesmo aponta o direito de retificação consagrado no artigo 16.º do *RGPD*.

III. Numa perspetiva económica, a possibilidade de se proceder ao tratamento de grandes quantidades de dados *(Big Data*[28]*)* revolucionou a forma de captação de novos clientes e de novos mercados, ao permitir, de forma particularmente fidedigna, traçar o perfil dos potenciais clientes, com todo o impacto decorrente nos processos de *marketing* e de publicidade[29].

O impacto da *Big Data* extravasa, largamente, o âmbito comercial e impõem-se hoje, com notáveis resultados, nos mais variados setores – p. ex.: na Política[30], na Saúde[31] ou na aplicação da Justiça[32].

---

[28] Ana Alves Leal, *Aspetos jurídicos da análise de dados na Internet (big data analytics) nos sectores bancário e financeiro: proteção de dados pessoais e deveres de informação em FinTech: Desafios da Tecnologia Financeira,* coord. António Menezes Cordeiro/Ana Perestrelo de Oliveira/Diogo Pereira Duarte, Almedina, Coimbra (2017), 75-203, 79 ss: sobre o conceito de *Big Data.*

[29] Sunil Erevelles/Nobuyuki Fukawa/Linda Swayne, *Big Data Consumer Analytics and the Transformation of Marketing,* 69 J Bus Res (2016), 897-904.

[30] Andrea Ceron/Luigi Curini/Stefano Maria Iacus, *Politics and Big Data,* Routledge: Londres (2016).

[31] Travis B. Murdoch/Allan S. Detsky, *The Inevitable Application of Big Data to Health Care,* JAMA, April 3, 2013 – Vol. 309, No. 13, 1351-1352.

[32] Lyria Bennett Moses/Janet Chan, *Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools,* 37 UNSWLJ (2014), 643-678.

IV. A amplitude do conceito de dado pessoal é reforçada pelo igualmente omnipresente conceito de tratamento de dado pessoal. O legislador avança com a sua definição no artigo 4.º, 2) do *RGPD*:

> [U]ma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

Esta definição legal decompõe-se em três elementos: (i) uma operação ou conjunto de operações; (ii) efetuadas sobre dados pessoais; e (iii) por meios automatizados ou não automatizados[33]. Nos termos do disposto no seu artigo 2.º/1, o *RGPD* apenas regula os tratamentos não automatizados, ou seja, operações que não envolvam equipamentos de processamento computadorizados de dados, que se encontrem contidos em ficheiros ou a eles se destinem[34].

O tratamento de dados pessoais apenas é considerado lícito na medida em que se encontre verificado um dos fundamentos elencados no artigo 6.º/1 do *RGPD*[35]: (a) o titular dos dados ter dado o seu consentimento; ser (b) para a execução de um contrato; (c) para o cumprimento de uma obrigação legal; (d) para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; (e) ao exercício de funções de interesse público ou ao exercício da autoridade pública; ou (f) para efeitos dos interesses legítimos pelo responsável pelo tratamento ou por terceiros.

---

(33) A. Barreto Menezes Cordeiro, Direito cit., 143 ss.

(34) A. Barreto Menezes Cordeiro, Direito cit., 86 ss.

(35) A. Barreto Menezes Cordeiro, Direito cit., 165 ss.

5. Os sujeitos do Direito da Proteção de Dados

I. O Direito da Proteção de Dados regula, *grosso modo,* a interação de três categorias de sujeitos: (i) os titulares dos dados; (ii) os responsáveis pelo tratamento; e (iii) eventualmente, os subcontratantes. Como se verifica nos demais Direitos privados regulados, a interação destes vários sujeitos é supervisionada por uma entidade independente, *in casu* denominada de autoridade de controlo: a Comissão Nacional de Proteção de Dados (CNPD).

II. O *RGPD* não contém uma definição de titular dos dados. O seu preenchimento é alcançado por intermédio do conceito de dados pessoais. Recupere-se o disposto no artigo 4.º, 1) do *RGPD*: "Dados pessoais", informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados")". Para efeitos do *RGPD*, apenas relevam os dados pessoais das pessoas singulares, sendo que apenas estas são incluídas no conceito de titular dos dados[36].

III. Por responsável pelo tratamento entende-se, nos termos do disposto no artigo 4.º, 7) do *RGPD*[37]:

> [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; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro.

---

(36) Considerando 14, p. 2 do *RGPD*: "O presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva".

(37) A. Barreto Menezes Cordeiro, *Direito* cit., 307 ss.

À luz desta definição e considerando que o TJUE tem sustentado uma interpretação ampla do conceito de responsável pelo tratamento, de modo a proteger os titulares dos dados[38], temos defendido que também os utilizadores de redes sociais são reconduzíveis a esta categoria, quando disponibilizam dados de terceiros – p. ex.: fotografias, imagens de vídeo ou informação relativa à vida privada[39].

Por fim, o subcontratante é um mandatário do responsável pelo tratamento: atua por conta deste último, 4.º, 8)[40]. O subcontratante será ainda, por maioria de razão, titular de uma posição fiduciária: está obrigado a atuar sempre no melhor interesse do beneficiário da relação – o responsável pelo tratamento[41].

A distinção entre as duas posições – responsável e subcontratante –, particularmente clara do ponto de vista teórico, suscita intensas dúvidas práticas. Na busca por esta distinção, importa atender aos seguintes indícios, que apontam para a pessoa responsável pelo tratamento: (i) utilização discricionária dos dados pessoais; (ii) junção de dados próprios aos dados que lhe foram transmitidos: (iii) aplicação dos dados transmitidos para propósitos próprios ou distintos dos originais; (iv) recolha de dados diretamente junto dos titulares; e (v) assunção de responsabilidades autónomas no tratamento dos dados.

---

(38) TJUE 13-mai.-2014, proc. C-131/12 *(Google Spain)*, 34; TJUE 5-jun.-2018, proc. C-210/16 *(Wirtschaftsakademie)*, 27-28; TJUE 29-jul.-2019, proc. C-40/17 *(Fashion ID)*, 66.

(39) A. Barreto Menezes Cordeiro, *Direitos de personalidade e dados pessoais: o que sobra para o Código Civil?*, VIII RDC (2023), 45-63, 54-55: com maiores desenvolvimentos.

(40) Artigo 1157.º do CC: "Mandato é o contrato pelo qual uma das partes se obriga a praticar um ou mais atos jurídicos por conta da outra".

(41) A. Barreto Menezes Cordeiro, *Relações fiduciárias: por uma doutrina unitária em Código Civil: Livro do Cinquentenário*, I, Almedina: Coimbra (2019), 25-47.

6. Os princípios do Direito da Proteção de Dados

I. O artigo 5.º do *RGPD* elenca um conjunto heterogéneo e transversal de princípios. A saber: (i) licitude; (ii) lealdade; (iii) transparência; (iv) limitação das finalidades; (v) minimização de dados; (vi) exatidão; (vii) limitação da conservação; (viii) integridade e confidencialidade; e (ix) responsabilidade.

Tratam-se de efetivos princípios, na aceção técnica do conceito: correspondem a valores jurídicos do sistema, que possibilitam a integração sistemática do Direito da Proteção de Dados e o preenchimento de eventuais lacunas identificadas pelo intérprete-aplicador.

II. *Ilicitude.* Em sentido estrito, o princípio da licitude faz depender o tratamento de dados pessoais da subsunção de cada tratamento em concreto a uma das causas de licitude elencadas no artigo 6.º. Em sentido amplo, pressupõe o cumprimento do *RGPD* e da demais legislação aplicável. Na primeira aceção respeita ao tratamento de dados e na segunda ao cumprimento da Lei[42].

Apesar de ambas as aceções serem corretas e relevantes, os termos licitude e ilicitude são, por princípio, utilizados no *RGPD* num sentido estrito, ou seja, a licitude do tratamento[43]. Esta interpretação é também suportada pelo artigo 8.º/2 da Carta: "... com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei".

---

[42] Considerando 40. Frenzel, *Anotação ao artigo 5.º do RGPD* em *Paal/Pauly Datenschutz-Grundverordnung – Bundesdatenschutzgesetz,* 2.ª ed., Beck: Munique (2018), Rn. 14; *Kühling/Buchner, Anotação ao artigo 5.º do RGPD* em *Kühling/Buchner Datenschutz-Grundverordnung, Bundesdatenschutzgesetz Kommentar,* 2.ª ed., Beck: Munique (2018), Rn. 8-9.

[43] Artigos 6.º, 7.º/3, 13.º/2, c) ou 14.º/2, d).

III. *Lealdade.* A lealdade representa um *plus* em relação ao princípio da licitude em sentido estrito. Neste sentido, a lealdade permite contestar determinados comportamentos que dificilmente poderiam ser descritos como violadores do artigo 6.º[44]. Trata-se de um conceito aberto[45], passível de ser invocado em situações que contradigam o espírito do *RGPD*.

É no âmbito das relações jurídicas que o princípio da lealdade irá encontrar o seu campo de aplicação por excelência[46]. A lealdade impõe aos responsáveis pelo tratamento a obrigação de atenderem, a todo o tempo, aos interesses e às expectativas legítimas dos titulares dos dados[47].

IV. *Transparência.* O princípio da transparência apresenta-se como uma novidade do *RGPD*[48]. As situações hoje reconduzíveis à transparência eram, durante a vigência da Diretriz n.º 95/46/CE, abrangidos pela lealdade[49]. A ligação entre os dois princípios é, de resto, manifesta: com o legislador europeu a emparelhar, sucessivamente, a lealdade e a transparência[50].

---

(44) Reimer, *Anotação ao artigo 5.º do RGPD* em *Sydow Europäische Datenschutzgrundverordnung Handkommentar*, 2.ª ed., Nomos: Baden-Baden (2018), Rn. 14.

(45) Buchner/Kühling, *Anotação ao artigo 5.º do RGPD em Kühling/Buchner* cit., Rn. 17: sublinhando a natureza aberta do termo.

(46) Heberlein, *Anotação ao artigo 5.º do RGPD em Ehmann/Selmayr, Datenschutz-Grundverordnung,* 2.ª ed., Beck: Munique (2018), Rn. 9; Roßnagel, *Anotação ao artigo 5.º do RGPD* em *Simitis/Hornung/Spiecker gen. Döhmann* cit., Rn. 44.

(47) Considerando 47, p. 1. Heberlein, *Anotação ao artigo 5.º do RGPD* em *Ehmann/Selmayr* cit., Rn. 9-10; Schantz, *Anotação ao artigo 5.º do RGPD* em *BeckOk Datenschutzrecht,* coord. Setfand Brink/Heinrich Amadeus Wolff, 28.ª ed., Beck: Munique, (2019), Rn. 8.

(48) Considerando 39; GT 29, *Orientações relativas à transparência na aceção do Regulamento 2016/679* (WP 260rev.1), 29-nov.-2017, revistas, por último, a 11-abr.-2018.

(49) TJUE 1-out.-2015, proc. c-201/14 *(Bara),* 34: "Daqui resulta que a exigência de tratamento leal dos dados pessoais prevista no artigo 6.º da Diretriz 95/46 obriga uma Administração Pública a informar as pessoas visadas da transmissão desses dados a outra Administração Pública, com vista ao seu tratamento por esta última, na sua qualidade de destinatária dos referidos dados"; Buchner/Kühling, *Anotação ao artigo 5.º do RGPD* em *Kühling/Buchner* cit., Rn. 18.

(50) Artigos 14.º/2 e 40.º/2, a) e Considerandos 60, p. 1 e 71, p. 5.

O princípio da transparência atravessa, horizontalmente, todo o processo de tratamento de dados, desde os primeiros contactos que o responsável pelo tratamento estabelece com potenciais titulares de dados (formação), passando pela sua recolha e demais tratamentos (execução), conservando-se mesmo após o termo da relação[51-52]. A transparência engloba tanto o conteúdo das informações a ser transmitidas aos titulares ou a terceiros, como os procedimentos da transmissão[53]. O princípio da transparência não se esgota no exercício do direito à informação dos titulares de dados pessoais[54].

Também o princípio da transparência surge concretizado em inúmeros artigos, com destaque para os artigos 12.º, 13.º e 14.º, mas também os artigos 34.º ou 37.º.

V. *Limitação das finalidades.* O disposto no artigo 5.º/1, b) limita a recolha de dados pessoais a finalidades (i) determinadas, (ii) explícitas e (iii) legítimas. O princípio da limitação de finalidades, previsto já na Diretriz n.º 95/46/CE, encontra o seu fundamento *constitucional* no artigo 8.º/2 da Carta – "fins específicos"[55]. A segunda parte do artigo 5.º/1, b) veda a prossecução subsequente de tratamentos de dados incompatíveis com as finalidades originariamente indicadas. Esta exigência visa, numa perspetiva geral, acautelar os interesses dos titulares e, numa perspetiva específica, garantir o controlo dos respetivos direitos à autodeterminação informacional[56].

---

(51) Como exemplo paradigmático, veja-se o artigo 17.º/2.

(52) GT 29, Orientações relativas à transparência cit., 6.

(53) Frenzel, *Anotação ao artigo 5.º do RGPD* em *Paal/Pauly* cit., Rn. 21; Heberlein, *Anotação ao artigo 5.º do RGPD* em *Ehmann/Selmayr* cit., Rn. 11.

(54) Roßnagel, *Anotação ao artigo 5.º do RGPD* em *Simitis/Hornung/Spiecker gen. Döhmann* cit., Rn. 50.

(55) Para uma análise às raízes históricas do princípio da limitação das finalidades: GP29, *Opinion 03/2013 on purpose limitations* (WP 203), 2-abr.-2013, 6 ss.

(56) Herbst, *Anotação ao artigo 5.º do RGPD* em *Kühling/Buchner* cit., Rn. 22.

VI. *Minimização de dados.* O princípio da minimização de dados[57] – artigo 5.º/1, c) – surge intrinsecamente associado ao princípio da limitação de finalidades: os dados pessoais devem ser "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados".

O princípio da minimização dos dados compõe-se de três pilares: (i) adequação; (ii) pertinência; e (iii) necessidade. Apesar de dificilmente autonomizáveis, em especial os dois primeiros, cada um visa propósitos distintos[58].

A adequação impõe a circunscrição dos tratamentos aos dados pessoais que se enquadrem nas finalidades prosseguidas. Os dados não relacionados ou inapropriados encontram-se, *ab initio*, excluídos[59].

A pertinência – o termo empregue na versão inglesa é mais feliz: *relevant* – circunscreve as atividades dos responsáveis a tratamentos que possam contribuir para a prossecução dessas finalidades.

Por fim, o tratamento apenas será juridicamente aceitável se não existir um método alternativo menos invasivo; p. ex.: a anonimização – 32.º/1, a) – ou a pseudonomização – 25.º/1.

VII. *Exatidão.* A alínea d) do artigo 5.º/1 abrange três dimensões: (i) a proibição de recolher ou armazenar dados incorretos; (ii) o dever de atualização dos dados detidos, sempre que se mostre necessário; e (iii) o dever de apagar ou de retificar os dados incorretos, à luz das finalidades prosseguidas[60].

A proibição de recolher e de armazenar dados incorretos circunscreve-se aos denominados dados objetivos e já não aos dados subjetivos[61].

---

(57) Este princípio é especialmente desenvolvido na anotação de Roßnagel, *Anotação ao artigo 5.º do RGPD* em *Simitis/Hornung/Spiecker gen. Döhmann* cit., Rn. 116 ss.

(58) Herbst, *Anotação ao artigo 5.º do RGPD* em *Kühling/Buchner* cit., Rn. 57.

(59) Heberlein, *Anotação ao artigo 5.º do RGPD* em *Ehmann/Selmayr* cit., Rn. 22.

(60) Schantz, *Anotação ao artigo 5.º do RGPD* em *BeckOk* cit., Rn. 34.

(61) Herbst, *Anotação ao artigo 5.º do RGPD* em *Kühling/Buchner* cit., Rn. 60.

A inexatidão dos dados pode ter um impacto enorme na vida dos seus titulares[62]. Contudo, nem todos os dados têm de estar, a todo o tempo, atualizados. De resto, alguns dados apenas têm interesse na medida, precisamente, em que se conservem desatualizados, por respeitarem a realidades passadas: pense-se em dados médicos que descrevem um estado clínico antigo. Por outro lado, a incorreção pode ser irrelevante para as finalidades prosseguidas, não afetando o tratamento ou os resultados que da sua análise decorram.

A obrigação de apagar ou de retificar dados incorretos não se confunde com os direitos a exigir o apagamento dos dados – independentemente de serem incorretos ou não, artigo 17.º – ou a sua retificação, artigo 16.º.

VIII. *Limitação da conservação.* A identidade dos titulares dos dados encontra-se, nos termos da alínea e) do artigo 5.º/1, temporalmente limitada às finalidades prosseguidas. Volvido o período de tempo necessário à sua conservação, devem ser, o quanto antes, apagados[63].

Nesse sentido, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou para a revisão periódica, de forma a assegurar que os dados pessoais sejam conservados apenas durante o período de tempo necessário.

A segunda parte do preceito consagra uma importante exceção a este princípio: os dados podem ser conservados por períodos temporais mais alargados se forem tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º/1. Cabe ao responsável, nestes casos, aplicar as medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados.

(62) TJUE 16-dez.-2008, proc. C-524/06 *(Huber)*, 60: dados relativos à situação pessoal do titular.

(63) TJUE 13-mai.-2014, proc. C-131/12 *(Google Spain)*, 73 e 92.

IX. *Integridade e confidencialidade.* A alínea f) do artigo 5.º/1 do *RGPD* impõe a obrigação de garantirem a segurança e a confidencialidade dos dados. A segurança abrange a perda, a destruição ou a danificação acidental, independentemente do impacto total ou parcial. Os responsáveis pelo tratamento devem adotar as medidas técnicas e organizativas adequadas a garantir o cumprimento de ambos os princípios.

IX. *Responsabilidade.* O artigo 5.º/2 consagra o princípio da responsabilidade: "o responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo".

O preceito prevê dois deveres distintos: (i) o responsável pelo tratamento deve atuar sempre no estrito cumprimento dos princípios elencados no artigo 5.º/1; e (ii) o responsável pelo tratamento deve conseguir demonstrar, *maxime* às autoridades de controlo e aos tribunais, o cumprimento desses mesmos princípios.

O princípio da responsabilidade – as expressões inglesas *accountability* e *compliance* transmitem uma ideia mais precisa do que efetivamente se pretende – assume uma função nuclear na estrutura e na aplicação do *RGPD*[64]. São inúmeros os preceitos que surgem ora como suas concretizações ou como suas decorrências lógicas: artigos 24.º/1, 30.º ou 33.º.

(64) O GT 29 desempenhou um papel decisivo na assunção, pelo legislador europeu, desta conceção: GT 29, *Opinion 3/2010 on the principle of accountability* (WP 173), 13-jul.-2010, 8 ss.

4 | A PROTEÇÃO DE DADOS PESSOAIS NA ÓTICA DO RESPONSÁVEL PELO TRATAMENTO À LUZ DO REGULAMENTO GERAL

*Alexandre L. Dias Pereira**

Sumário:

1. Introdução

A proteção dos dados pessoais funda-se no direito ao respeito pela vida privada consagrado na Declaração Universal dos Direitos Humanos de 1948 (Art.º 12.º), na Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais de 1950 (Art.º 8.º), e no Pacto Internacional dos Direitos Civis e Políticos de 1966 (Art.º 17.º). Portugal aderiu à Convenção Europeia dos Direitos Humanos em 1978, mas o Art.º 80.º do Código Civil já consagrava, como direito especial de personalidade, a reserva sobre a intimidade da vida privada[(65)],tal como sucederia com a Constituição da República Portuguesa (CRP) de 1976 (inicialmente no Art.º 33.º, passou na primeira reforma constitucional para o Art.º 26.º sobre direitos pessoais), a qual também limita quaisquer restrições a este

* Professor Associado da Faculdade de Direito da Universidade de Coimbra

(65) *Vd.* Orlando de Carvalho, «Les droits de l'homme dans le droit civil portugais », *Boletim da Faculdade de Direito da Universidade de Coimbra*, vol. 49 (1973), p. 1-24.

direito a casos e procedimentos previstos na lei e sujeitas a ordem judicial, e proíbe a ingerência das autoridades públicas na correspondência e nas telecomunicações, salvos os casos previstos na lei em matéria de processo criminal (Art.os 187.º a 190.º do Código de Processo Penal).

Todavia, a proteção de dados pessoais autonomizou-se do direito ao respeito pela vida privada, como dá conta a Carta de Direitos Fundamentais da União, que consagra o direito ao respeito pela vida privada e familiar no Art.º 7.º e o direito à proteção de dados pessoais no Art.º 8.º. Aliás, no direito interno, a nossa Constituição já destacara a proteção dos dados pessoais ao proibir a utilização da informática para tratar dados da vida privada das pessoas (Art.º 35.º).

A proteção dos dados pessoais corporiza um novo direito fundamental, designado «direito à autodeterminação informativa» no acórdão de 15 de dezembro de 1983 do *Bundesverfassungsgericht* (BVerfG)[(66)], num processo relativo a informações pessoais coletadas ao abrigo da Lei do Censo de 1983 (*Volkszählungsgesetzes* 1983), tendo o referido tribunal considerado que, no contexto do processamento moderno de dados, a proteção do indivíduo contra a recolha, armazenamento, uso e divulgação ilimitados dos seus dados pessoais é abrangida pelo direito fundamental de cada pessoa determinar a divulgação e o uso dos seus dados pessoais, sujeitando esta autodeterminação informacional apenas a limitações justificadas por razões de interesse público primordial[(67)].

---

(66) ECLI:DE:BVerfG:1983:rs19831215.1bvr020983: "1. No contexto do processamento de dados moderno, o direito geral de personalidade nos termos do Art.º 2.º, n.º 1, em conjugação com o Art.º 1.º, n.º 1, da Lei Básica, abrange a proteção do indivíduo contra a recolha, armazenamento, utilização e partilha ilimitadas dos seus dados pessoais. dados. Este direito fundamental confere ao indivíduo a autoridade para, em princípio, decidir ele próprio sobre a divulgação e utilização dos seus dados pessoais. / 2. As restrições deste direito à "autodeterminação informativa" só são permitidas se servirem um interesse público superior. Exigem uma base legal que deve ser constitucional e satisfazer o requisito de clareza jurídica no âmbito do Estado de direito. Na configuração do quadro legal, o legislador deve ainda observar o princípio da proporcionalidade. Deve também prever salvaguardas organizacionais e processuais que combatam o risco de violação do direito geral de personalidade. [...]" (tradução nossa).

(67) Vd. Paulo Mota Pinto, "O direito à reserva sobre a intimidade da vida privada", *Boletim da Faculdade de Direito da Universidade de Coimbra* vol. 64 (1993), p. 479-586; Alexandre Sousa Pinheiro, *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional*, Lisboa, AAFDL, 2015, passim.

Este direito fundamental foi recebido pela nossa doutrina constitucional ao abrigo do referido Art.º 35.º da Constituição, no sentido de o direito à autodeterminação informativa atribuir "a cada pessoa o direito de controlar a informação disponível a seu respeito" e de se impedir a redução da pessoa a mero "objeto de informação"4. A autodeterminação informativa confere à pessoa, por um lado, um "direito ao segredo (à intromissão dos outros na esfera privada, com tomada de conhecimento de aspetos a ela referentes)" e, por outro, "um direito à reserva (proibição de revelação)".

Este direito fundamental foi recebido pela nossa doutrina constitucional ao abrigo do referido Art.º 35.º da Constituição, no sentido de o direito à autodeterminação informativa atribuir "a cada pessoa o direito de controlar a informação disponível a seu respeito" e de se impedir a redução da pessoa a mero "objeto de informação"[68]. A autodeterminação informativa confere à pessoa, por um lado, um "*direito ao segredo* (à intromissão dos outros na esfera privada, com tomada de conhecimento de aspetos a ela referentes)" e, por outro, "*um direito à reserva* (proibição de revelação)"[69].

Por seu turno, a jurisprudência consagrou este novo direito fundamental em diversos acórdãos do Tribunal Constitucional[70], do Supremo Tribunal de Justiça[71] e dos Tribunais de Relação[72], o mesmo valendo

---

[68] J.J. Gomes Canotilho & Vital Moreira, *Constituição da República Portuguesa Anotada,* vol. 1, 4.ª ed., Coimbra, Coimbra Editora, 2007, p. 551.

[69] Joaquim de Sousa Ribeiro, "A tutela de bens da personalidade na Constituição e na jurisprudência constitucional portuguesas", in *Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho,* vol. III, Coimbra Editora, p. 853-859.

[70] Cf. acórdãos n° 442/2007, de 14 agosto de 2007, proc. n.º 815/2007 (considerando que o sigilo bancário não integra a esfera íntima da vida privada), acórdão n.º 403/2015, proc. 773/15, de 17 de setembro de 2015 (considerando o direito à autodeterminação informativa como manifestação, juntamente com o direito à solidão e o direito ao anonimato, do direito ao livre desenvolvimento da personalidade previsto no art.º 26 da CRP), n.º 268/2019, proc. 828/2019 e n.º 800/2023, proc. 1130/2023 (acesso a metadados referentes a comunicações eletrónicas para fins de investigação criminal).

[71] Cf. acórdão de uniformização de jurisprudência n.º 2/08, de 13 de fevereiro de 2008, proc. n.º 894/07-3, e acórdão de 16 de outubro de 2014, proc. no. 679/05.7TAEVR.E2.S1.

[72] Cf. acórdãos do Tribunal da Relação do Porto, de 31 de maio de 2006, proc. 0111584, do Tribunal da Relação de Coimbra, de 6 de abril de 2010, proc. 120-C/2000.C1, e do Tribunal da Relação de Évora, de 14 de setembro de 2017, proc. 2829/16.9T8PTM-B.E1.

para o Tribunal Europeu dos Direitos do Homem ao considerar no acórdão Satamedia que o Art.º 8.º da Convenção Europeia dos Direitos Humanos estabelece "o direito a uma forma de autodeterminação informacional" contra ingerências no exercício do seu direito à vida privada resultantes de recolha, processamento e disseminação pública dos seus dados pessoais[73].

A proteção de dados pessoais é atualmente objeto do Regulamento Geral de Proteção de Dados (*RGPD*)10, que regula a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e garante a liberdade de circulação de dados pessoais no interior da União Europeia (Art.º 1.º/1 e 3). A nível interno, a Lei de Proteção de Dados Pessoais (LPDP)[75] garante a execução do *RGPD* na ordem jurídica nacional. Este texto foca a proteção de dados pessoais na ótica do responsável pelo tratamento, o qual desempenha um papel central neste regime jurídico[76].

---

(73) *Satakunnan Markkinapörssi Oy and Satamedia Oy c. Finlândia* [GC], § 137, 27 de junho de 2017. Sobre o tema, Alexandre Dias Pereira, "66. Direito ao respeito pela vida privada digital", in *Comentário à Convenção Europeia dos Direitos Humanos e dos Protocolos Adicionais,* coord. Paulo Pinto de Albuquerque, Universidade Católica Editora, Lisboa, 2019, p. 1449-1470.

(74) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Doravante, salvo outra indicação, os artigos e considerandos citados são do *RGPD*.

(75) A Lei n.º 58/2019, de 8 de agosto, revogou a Lei n.º 67/98, de 26 de outubro, que transpunha a Diretiva 95/46/CE para a ordem jurídica interna.

(76) Vd. Alexandre Dias Pereira, "O responsável pelo tratamento de dados", Boletim da Faculdade de Direito da Universidade de Coimbra vol. 95/2 (2019), p. 1161-1188. Para comentários ao *RGPD* em língua portuguesa, vd. Comentário ao Regulamento Geral de Proteção de Dados, coord. Alexandre Sousa Pinheiro, Almedina, Coimbra, 2018; e Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019, coord. A. Barreto Menezes Cordeiro, Almedina, Coimbra, 2021. Sobre o impacto do *RGPD* no regime dos direitos de personalidade do Código Civil, vd. António Barreto Menezes Cordeiro, "Direitos de personalidade e dados pessoais: o que sobra para o Código Civil?", in Estudos em Homenagem ao Prof. Doutor António Pinto Monteiro, I. Direito Civil, Instituto Jurídico, Coimbra, 2023, p. 201-2017. Sobre a proteção de dados antes do *RGPD*, vd. inter alia Garcia Marques e Lourenço Martins, Direito da Informática, 2.ª ed., Coimbra, Almedina, 2006, p. 129-313, 422-442, 330-391; Helena Moniz, "Notas sobre a protecção de dados pessoais perante a informática: o caso especial dos dados pessoais relativos à saúde", Revista Portuguesa de Ciência Criminal 7/2 (1997), p. 231-298; Maria Eduarda Gonçalves, Direito da Informação - Novos Direitos e Formas de Regulação na Sociedade da Informação, 2.ª ed., Coimbra, Almedina, 2003, p. 82-111, 173-183; Catarina Sarmento e Castro, Direito da informática, privacidade e dados pessoais, Coimbra, Almedina, 2005.

Com efeito, o responsável pelo tratamento de dados pessoais é o destinatário principal dos deveres e obrigações estabelecidos no *RGPD*, e o responsável pelas coimas e outras sanções, que podem ser muito significativas (Art.os 83.º e 84.º). Por exemplo, o não cumprimento de uma ordem emitida pela autoridade de controlo (a CNPD em Portugal) fica sujeito a coimas até vinte milhões de euros ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante mais elevado (Art.º 83.º/6). Para além da responsabilidade pelo cumprimento dos princípios do tratamento de dados e do respeito pelos direitos dos seus titulares, o *RGPD* dedica especificamente o capítulo IV ao responsável pelo tratamento e ao subcontratante.

2. Noção de responsável pelo tratamento de dados pessoais

O responsável pelo tratamento tanto pode ser uma pessoa singular como uma pessoa coletiva, tanto de direito privado como de direito público, segundo a noção ampla prevista no *RGPD*: "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" (Art.º 4.º/7 *itálico nosso,* acrescentando, para efeitos de determinação do responsável pelo tratamento, que, "sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro").

Assim, o responsável pelo tratamento de dados pode ser uma pessoa de direito privado, singular ou coletiva (por ex. associação, fundação, sociedade civil ou comercial, cooperativa), ou uma autoridade pública, agência ou outro organismo (por ex. uma câmara municipal, uma universidade pública, uma agência de regulação, um hospital E.P.E., etc.). A natureza pública ou privada da entidade é irrelevante. O que conta é saber se a entidade em causa, isolada ou conjuntamente com outras entidades, determina as finalidades e os meios de tratamento

de dados, i.e., o para quê e o como. No caso de as *finalidades* e os *meios* de tratamento serem determinados conjuntamente por dois ou mais responsáveis, dá-se uma situação de *responsáveis conjuntos* pelo tratamento, respondendo todos solidariamente sem prejuízo do acordo de divisão interna de responsabilidades (Art.º 26.º).

Ao responsável pelo tratamento de dados junta-se o subcontratante, entendido como qualquer pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do primeiro (Art.º 4.º/8). Ambos realizam tratamento de dados, que é definido como "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (Art.º 4.º/2).

O operador de um sítio de comércio eletrónico é considerado responsável pelo tratamento de dados para efeitos do *RGPD* – como já antes tinha sido apontado, ao abrigo da Diretiva 95/46/CE[77] –, o mesmo valendo para o operador de motor de busca na *Internet:* "a atividade de um motor de busca que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, pô-las à disposição dos internautas por determinada ordem de preferência deve ser qualificada de «tratamento de dados pessoais», [...] quando essas informações contenham dados pessoais", devendo o operador desse motor de busca ser considerado "responsável" pelo dito tratamento[78].

---

[77] Cf. Grupo de trabalho do Art.º 29º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante,* WP 169, fevereiro de 2010.

[78] Acórdão de 13 de maio de 2014, proc. C-131/12, *Google Spain,* ECLI:EU:C:2014:317.

De igual modo, segundo o Tribunal de Justiça, o "administrador de um sítio *Internet,* como a *Fashion* ID [...], que insere no referido sítio um módulo social que permite ao navegador do visitante desse sítio solicitar conteúdos do fornecedor do referido módulo e transmitir para esse efeito a esse fornecedor dados pessoais do visitante, pode ser considerado responsável pelo tratamento", embora a responsabilidade seja "limitada à operação ou ao conjunto de operações de tratamento de dados pessoais cujas finalidades e meios são efetivamente determinados por esse administrador, a saber, a recolha e a comunicação por transmissão dos dados em causa"[79].

Além disso, relativamente ao utilizador de uma rede social em linha que consulta sítios Internet ou aplicações relacionados com uma ou várias das categorias de dados sensíveis, e, sendo caso disso, neles insere dados, registando-se ou efetuando encomendas em linha, o Tribunal de Justiça considerou como tratamento de categorias especiais de dados pessoais "o tratamento de dados pessoais pelo operador dessa rede social em linha, que consista na recolha, através de interfaces integradas, de cookies ou de tecnologias de registo semelhantes, dos dados resultantes da consulta desses sítios e dessas aplicações, bem como dos dados inseridos pelo utilizador, no cruzamento do conjunto desses dados com a conta da rede social desse utilizador e na utilização dos referidos dados por esse operador"[80].

De um modo geral, o responsável pelo tratamento de dados será, na grande maioria dos casos, uma pessoa coletiva, pública ou privada. Tanto mais que as atividades pessoais ou domésticas não são abrangidas pelo *RGPD*. Como se lê no considerando (18), o *RGPD* "não se aplica ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas e, portanto, sem qualquer ligação com uma atividade profissional ou comercial. As atividades pessoais ou domésticas poderão incluir a troca

[79] Acórdão de 29 de julho de 2019, C-40/17, Fashion ID, ECLI:EU:C:2019:629.

[80] Acórdão de 4 de julho de 2023, C-252/21, Meta Platforms, ECLI:EU:C:2023:537.

de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrónico no âmbito dessas atividades. Todavia, o presente regulamento é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas." Assim, por exemplo, os consumidores de redes sociais, como o *Facebook* ou o *Instagram,* não estão sujeitos ao *RGPD*, mas a empresa a quem pertencem, *Meta Platforms,* já é o responsável pelo tratamento de dados para efeitos legais.

A noção de responsável pelo tratamento de dados pessoais pressupõe a de dados pessoais, que significa "qualquer informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)", sendo "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" (Art.º 4.º/1). Nos termos do considerando (26), "Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica".

Os dados pessoais dizem respeito apenas a *pessoas singulares* e o *RGPD* cuida apenas dos dados de *pessoas vivas,* mas permite que os Estados-Membros estabeleçam regras para o tratamento dos dados de pessoas falecidas, como se lê no considerando (27). Lançando mão desta possibilidade, a LPDP estabelece a proteção dos dados pessoais de pessoas falecidas que se integrem nas "categorias especiais" de dados pessoais ou se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações (Art.º 17.º/1). Os direitos relativos a esses dados, nomeadamente os direitos de acesso, de retificação

e de apagamento, "são exercidos por quem a pessoa falecida haja designado para o efeito ou, na sua falta, pelos respetivos herdeiros" (Art.º 17.º/2), salvaguardando-se que os titulares dos dados podem determinar em vida a impossibilidade de exercício post-mortem desses direitos (Art.º 17.º/3).

Em todo o caso, trata-se apenas de dados de pessoas humanas ou físicas, já não de dados de pessoas coletivas, seja de direito privado (associações, fundações, sociedades civis ou comerciais) seja de direito público (Estado, regiões autónomas, autarquias locais, associações públicas, organismos autónomos, institutos públicos, entidades públicas empresariais, etc.).

3. Âmbito territorial de aplicação do *RGPD*

No que respeita ao âmbito territorial, o *RGPD* aplica-se a três grupos de casos. O primeiro grupo é constituído por tratamentos de dados pessoais efetuados no contexto das atividades de um estabelecimento de um responsável pelo tratamento de dados ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União (Art.º 3.º/1), considerando-se que o responsável com estabelecimentos em vários Estados-Membros tem estabelecimento principal no local onde se encontra a sua administração central na União, a menos que as decisões sobre as finalidades e os meios de tratamento dos dados pessoais sejam tomadas noutro estabelecimento do responsável pelo tratamento na União e este último estabelecimento tenha competência para mandar executar tais decisões, sendo neste caso considerando principal o que tiver tomado as referidas decisões (Art.º 4.º/16). Por ex., o acórdão *Google Spain*[81], o Tribunal de Justiça considerou que "é efetuado um tratamento de dados pessoais no contexto das atividades de um estabelecimento do responsável por esse tratamento no território de um Estado-Membro[...] quando o operador de um motor de busca cria num Estado-Membro uma sucursal ou uma filial destinada a assegurar

[81] Acórdão de 13 de maio de 2014, C-131/12, ECLI:EU:C:2014:317.

a promoção e a venda dos espaços publicitários propostos por esse motor de busca, cuja atividade é dirigida aos habitantes desse Estado-Membro".

No segundo grupo incluem-se os tratamentos de dados de titulares residentes no território da União, efetuados por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com a oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento, ou com o controlo do seu comportamento, desde que esse comportamento tenha lugar na União (Art.º 3.º/2-a). Para o efeito, segundo o considerando (23), "há que determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União. O mero facto de estar disponível na União um sítio *web* do responsável pelo tratamento ou subcontratante ou de um intermediário, um endereço eletrónico ou outro tipo de contactos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União." Por outro lado, ainda segundo o considerando (24), para "determinar se uma atividade de tratamento pode ser considerada «controlo do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes"[82].

[82] Sobre o tema, *vd.* António Pinto Monteiro e Sandra Passinhas, "Definição algorítmica de perfis e não discriminação dos consumidores", *Revista de Legislação e Jurisprudência,* n.º 4041, Ano 152.º (2023), p. 368-379.

Finalmente, no terceiro grupo são abrangidos, de acordo com o Art.º 3.º/3 interpretado à luz do considerando (25) do *RGPD*, os tratamentos efetuados por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público, por ex. no âmbito de uma missão diplomática ou num posto consular de um Estado-Membro.

4. Princípios do tratamento de dados pessoais

No leque de deveres a cargo do responsável pelo tratamento de dados sujeito ao *RGPD* surge à cabeça o de respeitar os princípios relativos ao tratamento de dados pessoais estabelecidos no *RGPD* (Art.º 5.º/1), a saber o princípio da licitude, lealdade e transparência, o princípio da limitação das finalidades, o princípio da minimização dos dados, o princípio da exatidão, o princípio da limitação da conservação, e o princípio da integridade e confidencialidade, além do princípio da responsabilidade pelo cumprimento desses princípios, que faz recair sobre o responsável o ónus da prova do cumprimento dos referidos princípios (Art.º 5.º/2), cabendo-lhe "provar que não é de modo algum responsável pelo evento que deu origem aos danos" (Art.º 82.º/3).

A licitude do tratamento pode resultar de vários fatores enumerados no Art.º 6.º/1, quais sejam: o consentimento do titular de dados, a necessidade do tratamento para a formação ou execução do contrato, o cumprimento de obrigação jurídica do responsável, a defesa de interesses vitais do titular ou de terceiro, o exercício de funções públicas ou autoridade pública do responsável, ou interesses legítimos do responsável ou de terceiro. Relativamente ao cumprimento de obrigação jurídica do responsável ou ao exercício de funções públicas ou autoridade pública do responsável, o fundamento jurídico deve estar previsto no direito da EU ou no direito nacional, o qual pode ter disposições específicas para adaptar a aplicação das regras do *RGPD*, como sejam, (a) as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento, (b) os tipos de dados objeto de tratamento, (c) os titulares dos

dados em questão, (d) as entidades a que os dados pessoais poderão ser comunicados e para que efeitos, (e) os limites a que as finalidades do tratamento devem obedecer, (f) os prazos de conservação, e (g) as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas relativas a outras situações específicas de tratamento (Art.º 6.º/3).

Assim, a justificação do tratamento não radica necessariamente no consentimento do titular dos dados. Como refere o *considerando* (46), "Alguns 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 ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana." Além disso, segundo o *considerando* (47), podem ser justificados por um interesse legítimo do responsável o "tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude", assim como "para efeitos de comercialização direta"[83]. Todavia, a cláusula do "interesse legítimo" não justifica à priori qualquer interesse do responsável pelo tratamento[84], tal como sustenta o Tribunal de Justiça *(vide infra)*[85].

---

(83) De acordo com o art.º 13.º/1 da Diretiva 2002/58/CE, a utilização de sistemas de chamada automatizados sem intervenção humana (aparelhos de chamada automáticos), de aparelhos de fax ou de correio eletrónico para fins de comercialização direta apenas poderá ser autorizada, em princípio, relativamente a assinantes que tenham dado o seu *consentimento prévio* ou em que, numa relação de clientela, o cliente não recuse a utilização dessas coordenadas para esses fins (para o direito interno, *vd.* art.º 13.º-A da Lei n.º 41/2004, de 18 de agosto).

(84) *Vd.* A. Barreto Menezes Cordeiro, «O tratamento de dados pessoais fundado em interesses legítimos», Revista de Direito e Tecnologia 1/1 (2019), p. 1-31.

(85) Acórdão de 4 de julho de 2023, C-252/21, ECLI:EU:2023:537, ponto 5.

5. A licitude do tratamento fundada no consentimento do titular dos dados

A licitude do tratamento funda-se, desde logo, no consentimento do titular dos dados, devendo o consentimento ser demonstrável, específico, livre e livremente revogável (Art.º 7.º). Não se exige um requisito de forma para o consentimento, valendo o princípio da liberdade de forma, como resulta do *considerando* (32): "O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio *web* na *Internet,* selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais." O consentimento pode ser expresso ou tácito, mas o silêncio do titular dos dados não vale como consentimento. Além disso, o eventual formulário do consentimento não pode onerar o titular com a necessidade de desautorizar um consentimento pré-definido, sendo cada consentimento vinculado apenas às finalidades de cada tratamento consentido. Ainda nos termos do referido *considerando* (32), "O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins."

Para ser livre, o consentimento não deve ser condição *sine qua non* de prestação de um serviço, se o tratamento de dados pessoais não for necessário para o efeito. Segundo o *considerando* (42), "uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, o titular dos

dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado"; a circunstância de não se poder consentir "separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico", ou de "a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução", essas circunstâncias fazem presumir que "o consentimento não é dado de livre vontade".

Por outro lado, na oferta direta de serviços da sociedade da informação[86] a crianças, o tratamento de dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos, embora os Estados-Membros possam reduzir para os 13 anos a idade mínima para consentir a utilização de dados pessoais neste domínio (Art.º 8.º), como sucedeu em Portugal (Art.º 16.º da LPDP), o que certamente não desagradará aos prestadores de serviços digitais, embora seja algo precoce esta espécie de «maioridade digital». Cabe ao responsável pelo tratamento implementar medidas técnicas de controlo da idade do menor, operação que envolverá, só por si, o tratamento de dados pessoais do menor.

6. A licitude do tratamento de categorias especiais de dados pessoais («dados sensíveis»)

Existem categorias especiais de dados cujo tratamento é proibido, salvo excecionalmente quando verificados determinados requisitos específicos. As categorias especiais abrangem dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas

[86] Por serviço da sociedade da informação entende-se "qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços", nos termos da Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação.

ou filosóficas, ou a filiação sindical de uma pessoa, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa (Art.º 9.º/1).

Assim, por exemplo, a proteção de interesses vitais justificará o tratamento de dados se o titular estiver incapaz de consentir. Por outro lado, é reservada aos Estados-Membros a possibilidade de manterem ou imporem novas condições, incluindo limitações, no que respeita ao tratamento de *dados genéticos,* dados biométricos ou dados relativos à saúde (Art.º 9.º/4). Os dados genéticos são definidos como "os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa" (Art.º 4.º/13). Os *dados biométricos* consistem em "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" (Art.º 4.º/14). Segundo o *considerando* (51), "O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular." Finalmente, os dados *relativos à saúde* são "os dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde" (Art.º 4.º/15). Na LPDP o tratamento de dados de saúde e genéticos é regulado pelo Art.º 29.º, e os dados biométricos pelo Art.º 28.º relativo ao tratamento de dados no âmbito de relações laborais.

O consentimento do titular é dispensado quando a lei autoriza o tratamento, nomeadamente por razões de proteção de interesses vitais do titular ou de terceiro, de interesse público, de formação ou execução de contratos, de interesses legítimos ou do cumprimento de obrigação legal (por ex., a videovigilância em certos estabelecimentos comerciais). No acórdão *Meta Platforms*[87], o Tribunal de Justiça pronunciou-se sobre alguns destes conceitos gerais relativamente ao tratamento de dados pessoais efetuado por um operador de uma rede social em linha, que consista na recolha de dados dos utilizadores dessa rede provenientes de outros serviços do grupo a que pertence esse operador ou provenientes da consulta por esses utilizadores de sítios Internet ou de aplicações de terceiros, no cruzamento desses dados com a conta da rede social dos referidos utilizadores e na utilização dos referidos dados.

Para começar, segundo o Tribunal, este tratamento "só pode ser considerado necessário para a *execução de um contrato* do qual os titulares de dados são partes, [...] *se esse tratamento for objetivamente indispensável para realizar uma finalidade que faça parte integrante da prestação contratual destinada a esses mesmos utilizadores,* de modo que o objeto principal do contrato não poderia ser alcançado sem esse tratamento"[88].

Depois, "só pode ser considerado necessário para efeitos dos *interesses legítimos* prosseguidos pelo responsável pelo tratamento ou por um terceiro, [...] desde que o referido operador tenha indicado aos utilizadores cujos dados foram recolhidos um interesse legítimo prosseguido pelo seu tratamento, que esse tratamento seja efetuado na *estrita medida do necessário* para a realização desse interesse legítimo e que resulte de uma *ponderação dos interesses opostos,* à luz de todas as circunstâncias pertinentes, que os interesses ou os direitos ou as liberdades fundamentais desses utilizadores não prevalecem sobre o referido interesse legítimo do responsável pelo tratamento ou de um terceiro"[89].

---

[87] Acórdão de 4 de julho de 2023, C-252/21, *Meta Platforms,* ECLI:EU:C:2023:537.

[88] *Idem,* ponto 4 *(itálico nosso).*

[89] Ibid., ponto 5 *(itálico nosso).*

Em terceiro lugar, o referido tratamento é justificado "quando for efetivamente necessário para o *cumprimento de uma obrigação jurídica* à qual o responsável pelo tratamento está sujeito, por força de uma disposição do direito da União ou do direito do Estado-Membro em causa, quando esse fundamento jurídico responda a um objetivo de interesse público e seja proporcionado ao objetivo legítimo prosseguido e quando esse tratamento seja efetuado na *estrita medida do necessário*"[90].

Finalmente, o referido tratamento "não pode, em princípio e sob reserva de verificação a efetuar pelo órgão jurisdicional de reenvio, ser considerado necessário à defesa de *interesses vitais* do titular dos dados ou de outra pessoa singular [...] ou ao exercício de funções de *interesse público* ou ao exercício da *autoridade pública* de que está investido o responsável pelo tratamento"[91].

7. Respeitar os direitos do titular dos dados, em especial o «direito a ser esquecido»

O responsável pelo tratamento de dados deve respeitar os direitos do titular de dados, começando pelo direito à *transparência* das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados (Art.º 12.º). Para o efeito o responsável deve prestar informações por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos, de forma concisa, transparente, inteligível e de fácil acesso, gratuita, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. O *RGPD* especifica as informações a facultar consoante os dados pessoais sejam ou não recolhidos junto do titular (Art.os 13.º e 14.º).

No exercício do direito de acesso, o titular dos dados deve poder saber que dados, para que fins, durante quanto tempo e de que modo, é feito o tratamento e a quem se destinam os dados (Art.º 15.º). O responsável pelo tratamento de dados fornece uma cópia dos dados pessoais em fase de tratamento e, para fornecer outras cópias solicitadas pelo titular

[90] Ibid., ponto 6 *(itálico nosso).*

[91] Ibid., ponto 7 *(itálico nosso).*

dos dados, pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrónico de uso corrente (Art.º 15.º/3). Segundo o *considerando* (63), "Quando possível, o responsável pelo tratamento deverá poder facultar o acesso a um sistema seguro por via eletrónica que possibilite ao titular aceder diretamente aos seus dados pessoais. [...] Quando o responsável proceder ao tratamento de grande quantidade de informação relativa ao titular dos dados, deverá poder solicitar que, antes de a informação ser fornecida, o titular especifique a que informações ou a que atividades de tratamento se refere o seu pedido".

São ainda direitos do titular de dados os direitos de retificação e de apagamento (Art.º 16.º e 17.º – "direito a ser esquecido"), o direito à limitação do tratamento (Art.º 18.º), o direito de portabilidade dos dados (Art.º 20.º)[92], o direito de oposição ao tratamento (Art.º 21.º) e o direito de não sujeição a decisões individuais automatizadas (Art.º 22.º). Os direitos do titular são limitados, nomeadamente por *razões de interesse público,* como se refere no considerando (71): "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, incluindo para efeitos de *controlo e prevenção de fraudes e da evasão fiscal,* conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para *garantir a segurança e a fiabilidade do serviço* prestado pelo 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" (itálicos nossos).*

[92] O direito à portabilidade encontra-se também no Regulamento 58/2005, de 18 de agosto, da ANACOM (alterado várias vezes), que estabelece os princípios e regras aplicáveis à portabilidade nas redes de comunicações públicas (Regulamento da Portabilidade), e no Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho de 14 de junho de 2017 relativo à portabilidade transfronteiriça dos serviços de conteúdos em linha no mercado interno. Sobre este direito vd. por ex. Vítor Palmela Fidalgo, "Art.º 20.º (Direito de portabilidade dos dados)", in Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019, coord. A. Barreto Menezes Cordeiro, Almedina, Coimbra, 2021, p. 204-213 e p. 594-6.

Por outro lado, o exercício destes direitos pelo titular gera obrigações para o responsável pelo tratamento de dados, nomeadamente, no que respeita à retificação ou ao apagamento, o dever de comunicar "a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais [...], salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado" (Art.º 19.º).

O "direito a ser esquecido" foi afirmado pelo Tribunal de Justiça no acórdão *Google Spain*[93], ao decidir que à luz dos Art.os 12.º/b) e 14.°/1-a) da Diretiva 95/46, "o operador de um motor de busca é obrigado a suprimir da lista de resultados, exibida na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, as ligações a outras páginas *web* publicadas por terceiros e que contenham informações sobre essa pessoa, também na hipótese de esse nome ou de essas informações não serem prévia ou simultaneamente apagadas dessas páginas *web,* isto, se for caso disso, mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita." Mais acrescentou que o referido direito não pressupõe que "a inclusão dessa informação nessa lista causa prejuízo a essa pessoa", cujos direitos à vida privada e à proteção de dados pessoais, consagrados nos Art.os 7.º e 8.º da Carta de Direitos Fundamentais da União, "prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em aceder à informação numa pesquisa sobre o nome dessa pessoa", salvo "se se afigurar que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão, em virtude dessa inclusão".

---

[93] Acórdão de 13 de maio de 2014, proc. C-131/12, *Google Spain,* ECLI:EU:C:2014:317. Defendendo que se trata antes de um "direito à desassociação" nos motores de pesquisa na internet, Filipa Calvão, "A proteção de dados pessoais na internet: desenvolvimentos recentes", *Revista de Direito Intelectual* N.º 2 - 2015, p. 67-84. O direito ao esquecimento, enquanto "direito geral de eliminação de dados pessoais", em especial na *Internet,* não terá equivalente nos EUA, *vd.* Dário Moura Vicente e Sofia de Vasconcelos Casimiro, "A proteção de dados pessoais na *Internet* à luz do Direito Comparado", *Revista de Direito Intelectual*, N.º 2 - 2018, p. 45-90, 67.

Posteriormente, relativamente ao âmbito territorial do direito ao esquecimento, o Tribunal concluiu no acórdão *Google c. CNIL*[94] que "*o operador de um motor de busca não tem de efetuar [a] supressão de referências em todas as versões do seu motor,* devendo fazê-lo nas versões deste que correspondem a todos os Estados-Membros, e isto, se necessário, em conjugação com medidas que, embora satisfaçam as exigências legais, permitam efetivamente impedir ou, pelo menos, desencorajar seriamente os internautas que efetuam uma pesquisa a partir do nome da pessoa em causa dentro de um dos Estados-Membros de, através da lista de resultados exibida após essa pesquisa, aceder às hiperligações que são objeto desse pedido".

Ainda a propósito do "direito ao esquecimento", o Tribunal de Justiça decidiu, no acórdão do TU/TE c. *Google*[95], que "a supressão de referências dirigido ao operador de um motor de busca e destinado a suprimir da lista de resultados de uma pesquisa a hiperligação para um conteúdo que contém alegações que a pessoa que apresentou o pedido considera inexatas[...] *não está sujeita à condição de que a questão da exatidão do conteúdo apresentado tenha sido resolvida, pelo menos provisoriamente,* no âmbito de uma ação intentada por essa pessoa contra o fornecedor de conteúdos", ressalvando, todavia, que estando em causa "suprimir resultados de uma pesquisa de imagens, efetuada a partir do nome de uma pessoa singular, as fotografias, exibidas sob a forma de imagens de pré-visualização, que representam essa pessoa, deve ter-se em conta o valor informativo dessas fotografias independentemente do contexto da sua publicação na página Internet da qual foram retiradas, mas tendo em consideração todos os elementos textuais que acompanhem diretamente a exibição das referidas fotografias nos resultados de pesquisa e que sejam suscetíveis de elucidar o valor informativo das mesmas".

Na outra face do direito ao esquecimento encontra-se o dever de conservação dos dados a cargo do responsável pelo tratamento. Nos termos do Art.º 21.º da LPDP, o prazo de conservação de dados pessoais é "o que

(94) Acórdão de 24 de setembro, proc. C-507/17, *Google c. CNIL,* ECLI:EU:C:2019:772.

(95) Acórdão de 8 de dezembro de 2022, C-460/20, TU/RE c. Google, ECLI:EU:C:2022:962.

estiver fixado por norma legal ou regulamentar ou, na falta desta, o que se revele necessário para a prossecução da finalidade, considerando-se lícita a conservação dos dados pessoais, desde que sejam adotadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados, designadamente a informação da sua conservação, quando, pela natureza e finalidade do tratamento, designadamente para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos, não seja possível determinar antecipadamente o momento em que o mesmo deixa de ser necessário, ou enquanto não decorrer o prazo de prescrição dos direitos contratuais por parte do RTD ou do subcontratante. Decorrido esse prazo ou cessada a finalidade que motivou o tratamento, inicial ou posterior, o responsável pelo tratamento tem o dever de destruir ou de anonimizar os dados pessoais, e o direito ao apagamento só pode ser exercido depois de decorrido o prazo legal imperativo de conservação dos dados.

Os prazos de prescrição de dívidas, que justificam a conservação dos dados pessoais durante esse período, são, segundo o Código Civil, desde 6 meses para os serviços públicos essenciais como água, gás, eletricidade e telecomunicações; estabelecimentos de alojamento, restauração e afins (Art.º 316.º), até 20 anos, que é o prazo ordinário das dívidas contratuais (Art.º 309.º), passando por 2 anos para dívidas de alojamento e alimentação de estudantes, estabelecimentos de ensino e de saúde, dívidas de consumidores a comerciantes e a profissionais liberais (Art.º 317.º), 5 anos para prestações periodicamente renováveis, como rendas, juros ou pensões de alimentos e dividendos (Art.º 310.º do Código Civil), e 8 anos para as propinas do ensino superior (Art.º 48.º da Lei Geral Tributária).

Não obstante, a lei ressalva a licitude de conservação sem limite de prazo de dados relativos a declarações contributivas para efeitos de aposentação ou reforma a fim de auxiliar o titular na reconstituição das carreiras contributivas, desde que sejam adotadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados (Art.º 21.º/6 LPDP).

8. Aplicar medidas técnicas e organizativas adequadas ao risco, desde a conceção e por defeito, em especial segundo códigos de conduta ou procedimentos de certificação

O responsável pelo tratamento de dados deve aplicar *medidas técnicas e organizativas adequadas ao risco* (consoante a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares) para assegurar e comprovar a conformidade do tratamento com o *RGPD*, devendo revê-las e atualizá-las consoante as necessidades (Art.º 24.º). As medidas técnicas e organizativas adequadas, como a *pseudonimização* e a cifragem de dados, devem ser implementadas a fim de a proteção de dados ocorrer *desde a conceção e por defeito.* Por exemplo, essas medidas devem assegurar, por defeito, a não disponibilização dos dados sem intervenção humana a um número indeterminado de pessoas singulares (Art.º 25.º/1-2).

De igual modo, o responsável pelo tratamento só pode recorrer a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas a cumprir o *RGPD* e que respeitem os direitos do titular dos dados (Art.º 28.º). As medidas técnicas e organizativas devem ser adequadas ao risco, para assegurar a confidencialidade, a integridade, a disponibilidade e a resiliência permanentes dos sistemas e dos serviços de tratamento, devendo dispor de um processo para testar, apreciar e avaliar regularmente a eficácia dessas medidas (Art.º 32.º).

O cumprimento desta obrigação pode fazer-se através de códigos de conduta ou procedimentos de certificação aprovados nos termos do *RGPD* (Art.º 42.º)[96] Segundo o considerando (77), "As orientações sobre

[96] O regime jurídico da cibersegurança foi aprovado pela Lei n.º 46/2018, de 13 de agosto, que transpõe a Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, a qual foi revogada pela Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022. Sobre o tema, *vd.* Alexandre Dias Pereira, "Proteção do consumidor e segurança informática no comércio eletrónico", *Revista Bolsa, Banca e Seguros* 3 (2018), p. 303-329.

a execução de medidas adequadas e sobre a comprovação de conformidade pelos responsáveis pelo tratamento ou subcontratantes, em especial no que diz respeito à identificação dos riscos relacionados com o tratamento, à sua avaliação em termos de origem, natureza, probabilidade e gravidade, bem como à identificação das melhores práticas para a atenuação dos riscos, poderão ser obtidas nomeadamente recorrendo a códigos de conduta aprovados, a certificações aprovadas, às orientações fornecidas pelo Comité ou às indicações fornecidas por um encarregado da proteção de dados".

As associações de responsáveis pelo tratamento de dados elaboram códigos de conduta (Art.º 40.º), cuja supervisão "pode ser efetuada por um organismo que tenha um nível adequado de competência relativamente ao objeto do código e esteja acreditado para o efeito pela autoridade de controlo competente" (Art.º 41.º). Além disso, os responsáveis pelo tratamento podem cumprir *procedimentos de certificação* em matéria de proteção de dados, bem como adotar selos e marcas de proteção de dados, para efeitos de comprovação da conformidade dos tratamentos com o *RGPD* (Art.º 42.º). A certificação, válida em princípio por três anos, é efetuada por organismo de certificação acreditado pela autoridade de controlo ou diretamente por esta (Art.º 43). Em Portugal, o IPAC I.P é a autoridade competente para a acreditação dos organismos de certificação em matéria de proteção de dados, ao passo que a elaboração de códigos de conduta que regulem atividades determinadas compete à CNDP, atendendo às necessidades específicas das micro, pequenas e médias empresa (Art.º 14.º da LPDP).

9. Encarregado de proteção de dados (EPD/DPO) e representante na União

O responsável pelo tratamento de dados deve designar um encarregado de proteção de dados (EPD) – *Data Protection Officer* (DPO) – se for uma autoridade ou um organismo público (podendo o encarregado ser comum a vários organismos ou autoridades, tendo em conta a respetiva estrutura organizacional e dimensão), ou exercer atividade que exija o controlo de titulares de dados ou o tratamento de dados em

grande escala (Art.º 37.º). Segundo as *Orientações do Grupo de Trabalho do Art.º 29.º*[97], consideram-se de grande escala: "o tratamento de dados de doentes no exercício normal das atividades de um hospital; tratamento de dados de viagem das pessoas que utilizam o sistema de transportes públicos de uma cidade (p. ex., através de passes de viagem); o tratamento em tempo real de dados de geolocalização de clientes de uma cadeia de restauração rápida internacional para fins estatísticos por parte de um subcontratante especializado na prestação desses serviços; o tratamento de dados de clientes no exercício normal das atividades de uma companhia de seguros ou de um banco; o tratamento de dados pessoais para fins de publicidade comportamental por um motor de busca; o tratamento de dados (conteúdo, tráfego, localização) por operadoras telefónicas ou por fornecedores de serviços de *internet*". Pela negativa, não são de grande escala os tratamentos de dados de pacientes por um médico e os de dados pessoais relacionados com condenações penais e infrações por um advogado.

Sendo um grupo empresarial, o responsável pelo tratamento de dados pode designar um único EPD/DPO se ele for facilmente acessível a partir de cada estabelecimento (Art.º 37.º/2)[98]. O responsável pelo tratamento de dados deve publicar os contactos do Encarregado e comunicá-los à autoridade de controlo, e deve apoiar o encarregado e respeitar a

---

[97] Grupo de Trabalho do Art.º 29.º para a Proteção de Dados, *Orientações sobre os encarregados da proteção de dados (EPD).* Adotadas em 13 de dezembro de 2016, com a última redação revista e adotada em 5 de abril de 2017, WP 243 rev.01, p. 10.

[98] Para efeitos do *RGPD*, a noção de empresa abrange "uma pessoa singular ou coletiva que, independentemente da sua forma jurídica, exerce uma atividade económica, incluindo as sociedades ou associações que exercem regularmente uma atividade económica" (art.º 4.º/18); por grupo empresarial entende-se "um grupo composto pela empresa que exerce o controlo e pelas empresas controladas" (art.º 4.º/19). Segundo o considerando (22), "A forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto". Por outro lado, segundo o considerando (36), "A existência e utilização de meios técnicos e de tecnologias para o tratamento de dados pessoais ou as atividades de tratamento não constituem, em si mesmas, um estabelecimento principal nem são, portanto, um critério definidor de estabelecimento principal. [...] Sempre que o tratamento dos dados seja efetuado por um grupo empresarial, o estabelecimento principal da empresa que exerce o controlo deverá ser considerado o estabelecimento principal do grupo empresarial, exceto quando as finalidades e os meios do tratamento sejam determinados por uma outra empresa".

sua autonomia no desempenho das suas funções de zelar pelo cumprimento do *RGPD*, que pode cumular com outras funções e atribuições que não resultem num conflito de interesses (Art.º 38.º/6). No direito interno, o Art.º 9.º da LPDP estabelece que a designação de EPD não depende de certificação profissional da pessoa em causa, a qual exerce a sua função com autonomia técnica perante a entidade responsável pelo tratamento ou subcontratante, independentemente da natureza da sua relação jurídica (laboral ou prestação de serviços). Nos termos do *RGPD*, cabe ao responsável pelo tratamento assegurar que o EPD "não recebe instruções relativamente ao exercício das suas funções" e que "não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções" (Art.º 38.º/3). De todo o modo, não é dever do EPD/DPO denunciar eventuais infrações cometidas pelo responsável pelo tratamento de dados à autoridade de controlo[99].

Os responsáveis pelo tratamento ou os subcontratantes que não estejam estabelecidos na União devem designar, por escrito, um representante na União, salvo se forem atividades ocasionais e que não envolvam o tratamento em grande escala de dados sensíveis, ou realizadas por autoridades ou organismos públicos (Art.º 27.º). Por *representante* entende-se "uma pessoa singular ou coletiva estabelecida na União que, designada por escrito pelo responsável pelo tratamento ou subcontratante, nos termos do Art.º 27º, representa o responsável pelo tratamento ou o subcontratante no que se refere às suas obrigações respetivas nos termos do" *RGPD* (Art.º 4.º /17). Nos termos do *considerando* (80), *"O representante deverá ser explicitamente designado por um mandato do responsável pelo tratamento ou subcontratante, emitido por escrito,* que permita ao representante agir em seu nome no que diz respeito às obrigações que lhes são impostas pelo presente regulamento" *(itálico nosso).*

(99) Cf. *Orientações do Grupo de Trabalho do art.º 29.º sobre o Encarregado de Proteção de Dados,* cit., p. 21. Sobre a compatibilidade entre a autonomia do EPD e a independência do Advogado, vd. A. Barreto Menezes Cordeiro, "A Autonomia da Função de Encarregado de Proteção de Dados e a Independência do Exercício da Advocacia", *Revista da Ordem dos Advogados* 78/I-II (2018), p. 17-38.

10. Registar os tratamentos sob sigilo

O responsável pelo tratamento de dados deve manter um registo escrito de todas as atividades de tratamentos efetuados, especificando as informações como o seu nome e contactos, e do seu representante ou do encarregado de proteção de dados (EPD/DPO), as finalidades do tratamento, as categorias de titulares de dados, os dados pessoais, e os destinatários, as transferências, os prazos de apagamento dos dados, e a descrição das medidas técnicas e organizativas de segurança (Art.º 30.º). Ficam isentos deste dever os responsáveis pelo tratamento de dados com menos de 250 trabalhadores, a menos que tratem "dados sensíveis" ou relativos a condenações penais (Art.º 30.º/5). O modelo de registo das atividades de tratamento previsto no Art.º 30.º da LPDP está disponível no sítio da CNPD[100].

O *RGPD* não prejudica a obrigação de sigilo a que o responsável pelo tratamento de dados esteja sujeito, por força de lei interna do Estado-membro, relativamente aos dados pessoais que tenha recebido no âmbito de uma atividade abrangida por essa obrigação de sigilo ou em resultado da mesma (Art.º 90.º). Por ex., o Regulamento de Deontologia Médica[101] encarrega os responsáveis pelo tratamento da informação de saúde de tomarem as "providências adequadas à proteção da sua confidencialidade, garantindo a segurança das instalações e equipamentos, o controlo no acesso à informação, bem como o reforço do dever de sigilo e da educação deontológica de todos os profissionais" (Art.º 37.º). O dever de confidencialidade da informação de saúde é reiterado no capítulo VII do Regulamento sobre a telemedicina (Art.os 46.º a 49.º)[102].

---

(100) *Vd.* https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/.

(101) Regulamento n.º 707/2016, de 21 de julho.

(102) Sobre o tema vd. por ex. Filipe Miguel Cruz de Albuquerque Matos, "O Regulamento de Protecção de Dados Pessoais (2016/679) no contexto dos desafios da actividade seguradora — o caso particular dos seguros de saúde", *Revista Bolsa, Banca e Seguros* 3 (2018), p. 51-122; Alexandre Dias Pereira, "A proteção dos dados pessoais no direito português, em especial no setor da saúde", in *Algunos desafios en la proteccion de datos personales,* org. Alfredo Batuecas Caletrio, Juan Pablo Aparicio Vaquero, Comares, Madrid, 2018.

A lei interna sujeita a um dever de confidencialidade, "que acresce aos deveres de sigilo profissional previsto na lei, não apenas o encarregado de proteção de dados e os responsáveis pelo tratamento e os subcontratantes, mas também "todas as pessoas que intervenham em qualquer operação de tratamento de dados" (Art.º 10.º/2 LPDP).

11. Cooperar com a autoridade de controlo, notificar violações de dados e avaliar o impacto do tratamento de dados pessoais

O responsável pelo tratamento de dados deve cooperar com a autoridade de controlo (Art.º 31.º). Em especial, deve notificar, em princípio no máximo de 72 horas, uma violação de dados pessoais à autoridade de controlo (Art.º 33.º). Se a violação de dados pessoais implicar um elevado risco para os direitos e liberdades das pessoas singulares, deve comunicar esse facto ao titular dos dados, a menos que tenha usado técnicas como a cifragem (Art.º 34.º).

Por outro lado, o responsável pelo tratamento de dados deve avaliar o impacto sobre a proteção de dados por ex. em caso de tratamento sistemático de dados sensíveis em larga escala (Art.º 35.º). Nos termos do considerando (91), "O tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado. Nesses casos, a realização de uma avaliação de impacto sobre a proteção de dados não deverá ser obrigatória." Todavia, a referência ao "hospital" juntamente com os profissionais de saúde isentos do dever de avaliação de impacto resulta manifestamente de um lapso de redação da versão portuguesa do *RGPD*, como se constata facilmente, comparando-a com as versões inglesa, francesa ou castelhana.

Se concluir que o tratamento envolve um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento de dados deve proceder a consulta prévia à autoridade de controlo (Art.º 36.º). O *RGPD* ressalva que a lei interna de cada Estado-Membro pode inclusivamente sujeitar a autorização prévia da autoridade de

controlo o tratamento por um responsável no exercício de uma missão de interesse público, incluindo o tratamento por motivos de proteção social e de saúde pública (Art.º 36.º/5). Em Portugal, a autoridade de controlo é a Comissão Nacional de Proteção de Dados, a qual, no exercício das suas atribuições legais, estabeleceu uma lista de operações sujeitas a avaliação de impacto[103], incluindo designadamente: a utilização de dispositivos eletrónicos que transmitam, por redes de comunicação, dados pessoais relativos à saúde (apps de saúde); a criação de perfis em grande escala, ou rastreamento da localização ou dos comportamentos dos respetivos titulares (por exemplo, trabalhadores, clientes ou apenas transeuntes), que tenha como efeito a avaliação ou classificação destes, exceto quando o tratamento seja indispensável para a prestação de serviços requeridos especificamente pelos mesmos; e o tratamento de dados biométricos para identificação inequívoca dos seus titulares, ou de dados genéticos, quando estes sejam pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados. Além disso, a lei interna exige autorização prévia da CNPD para a captação de som na videovigilância, quando esta é admitida, exceto no período em que as instalações vigiadas estejam encerradas (Art.º 19.º/4 LPDP).

12. Transferência de dados para fora da União Europeia

Um dos objetivos do *RGPD* é garantir a livre circulação de dados pessoais no interior no mercado interno. O regime anteriormente em vigor, no quadro da Diretiva 95/46/CE, permitiu diferenças significativas entre os níveis de proteção a nível nacional, em virtude de disparidades na transposição da referida Diretiva, com prejuízo para o exercício de atividades económicas e para a concorrência no mercado interno. Nesse sentido,

[103] O Regulamento n.º 798/2018 da CNPD estabelece a lista de operações sujeitas a avaliação de impacto. Sobre a avaliação de impacto, *vd.* Grupo de Trabalho do Art.º 29.º para a Proteção de Dados, *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679*, adotadas em 4 de abril de 2017, revistas e adotadas pela última vez em 4 de outubro de 2017, WP 248 rev.01.

como se lê no considerando (10), "É conveniente assegurar em toda a União a aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais".

Não obstante – *et pour cause* –, as transferências de dados para fora da União Europeia já são rodeadas das maiores cautelas, tanto mais que no ciberespaço as fronteiras territoriais são pouco nítidas, sendo difícil assegurar que os dados pessoais dos cidadãos residentes na União Europeia beneficiem de um elevado nível de proteção extramuros. Nesse sentido, o responsável pelo tratamento só pode transferir dados pessoais para países terceiros ou organizações internacionais se atuar em conformidade com o *RGPD* (Art.º 44.º), designadamente com base numa decisão da Comissão de adequação do nível de proteção do país terceiro (Art.º 45.º)[104] Na falta de uma tal decisão de adequação, a transferência pode ocorrer se o responsável pelo tratamento apresentar garantias adequadas e os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes (Art.º 46.º). Essas garantias adequadas podem resultar, por exemplo, de regras vinculativas aplicáveis às empresas (Art.º 47.º)[105], de cláusulas-tipo de proteção de dados adotadas ou aprovadas pela Comissão[106], de código de conduta ou procedimento de certificação, acompanhados de compromissos vinculativos e com força executiva, como informa o *considerando* (108).

---

[104] Na sequência do acórdão de 16 de julho de 2020, C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd e Maximillian Schrems,* ECLI:EU:C:2020:559, no qual o Tribunal de Justiça declarou a invalidade da Decisão da Comissão Europeia n.º 2016/1250 que implementou o «Privacy Shield Framework», destinado a facilitar as transferências internacionais de dados pessoais da UE para os Estados Unidos da América, foi aprovado um novo protocolo: Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, Brussels, 10.7.2023 C(2023) 4745 final. Em matéria de legislação estadual, destaca-se a *California Consumer Privacy Act* de 2018 (<https://oag.ca.gov/privacy/ccpa>), sendo que a maioria das grandes empresas da Internet está estabelecida neste Estado norte-americano.

[105] *Vd.* Grupo de Trabalho do Art.º 29.º para a Proteção de Dados, *Documento de trabalho que cria uma tabela com os elementos e os princípios que constam das regras vinculativas para as empresas.* Adotado em 28 de novembro de 2017, última redação revista e adotada em 6 de fevereiro de 2018, WP 256 rev. 01.

[106] *Vd.* Decisão de Execução (UE) 2021/914 da Comissão, de 4 de junho de 2021, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho.

Além disso, mesmo na ausência de uma decisão de adequação ou de garantias adequadas (por ex. regras vinculativas aplicáveis às empresas), as transferências para países terceiros podem ser efetuadas para situações específicas, nomeadamente se houver consentimento explícito e informado do titular dos dados, se a transferência for necessária em sede contratual ou por razões de interesse público ou para proteger interesses vitais de pessoa incapaz de consentir, para além de outras derrogações para situações específicas previstas no Art.º 49.º.

No acórdão *Schrems*[107] o Tribunal de Justiça decidiu, em primeiro lugar, que o *RGPD* se aplica a "uma transferência de dados pessoais efetuada para fins comerciais por um operador económico estabelecido num Estado-Membro para outro operador económico estabelecido num país terceiro, não obstante o facto de, no decurso ou na sequência dessa transferência, esses dados serem suscetíveis de ser tratados pelas autoridades do país terceiro em causa para efeitos de segurança pública, de defesa e de segurança do Estado". Em segundo lugar, o Tribunal decidiu que "as garantias adequadas, os direitos oponíveis e as medidas jurídicas corretivas eficazes, [...] devem assegurar que os direitos das pessoas cujos dados pessoais são transferidos para um país terceiro com base em cláusulas-tipo de proteção de dados beneficiam de um nível de proteção substancialmente equivalente ao garantido na União Europeia por este regulamento, lido à luz da Carta dos Direitos Fundamentais da União Europeia. Para este efeito, a avaliação do nível de proteção assegurado no contexto dessa transferência deve, nomeadamente, ter em consideração tanto as estipulações contratuais acordadas entre o responsável pelo tratamento ou o seu subcontratante estabelecidos na União Europeia e o destinatário da transferência estabelecido no país terceiro em causa como, no que respeita a um eventual acesso das autoridades públicas desse país terceiro aos dados pessoais assim transferidos, os elementos pertinentes do sistema jurídico deste país terceiro, nomeadamente os enunciados no Art.º 45.º, n.º 2, do *RGPD*", designadamente o primado do Estado de direito e o respeito pelos direitos humanos e liberdades fundamentais.

[107] Acórdão de 16 de julho de 2020, C-311/18, *Facebook* e *Maximillian Schrems,* ECLI:EU:C:2020:559.

Finalmente, o Tribunal determinou que "a menos que exista uma decisão de adequação validamente adotada pela Comissão Europeia, a autoridade de controlo competente está obrigada a suspender ou a proibir uma transferência de dados para um país terceiro com base em cláusulas-tipo de proteção de dados adotadas pela Comissão, se essa autoridade de controlo considerar, à luz de todas as circunstâncias específicas dessa transferência, que essas cláusulas não são ou não podem ser respeitadas nesse país terceiro e que a proteção dos dados transferidos exigida pelo direito da União, em particular pelos Art.os 45.º e 46.º deste regulamento e pela Carta dos Direitos Fundamentais, não pode ser assegurada por outros meios, no caso de o responsável pelo tratamento ou o seu subcontratante estabelecidos na União não terem eles próprios suspendido ou posto termo à transferência".

13. Derrogações ao regime geral de tratamento de dados

A liberdade de expressão e de informação, incluindo o tratamento para fins jornalísticos e para fins de expressão académica, artística ou literária, justifica derrogações específicas ao regime geral de tratamento de dados (Art.º 85.º). Na lei interna, a proteção de dados pessoais não prejudica o exercício da liberdade de expressão, informação e imprensa, incluindo o tratamento de dados para fins jornalísticos e para fins de expressão académica, artística ou literária, salvaguardado o princípio da dignidade da pessoa humana previsto na Constituição e os direitos de personalidade. De todo o modo, o tratamento para fins jornalísticos só pode ser feito por jornalistas reconhecidos como tais, segundo o regime de acesso e exercício da profissão, e, em qualquer caso o exercício da liberdade de expressão não legitima a divulgação de dados pessoais como moradas e contactos, à exceção daqueles que sejam de conhecimento generalizado (Art.º 24.º LPDP).

De igual modo, são previstas derrogações para o "tratamento e acesso do público aos documentos oficiais" (Art.º 86.º)[108], o "tratamento do número de identificação nacional" (Art.º 87.º), o "tratamento no contexto laboral" (Art.º 88.º)[109], e o "tratamento para fins de arquivo de interesse

(108) O acesso ao documentos administrativos é regulado pela Lei de Acesso aos Documentos da Administração, Lei n.º 26/2016, de 22 de agosto, que aprova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos, transpondo a Diretiva 2003/4/CE, do Parlamento Europeu e do Conselho, de 28 de janeiro, e a Diretiva 2003/98/CE, do Parlamento Europeu e do Conselho, de 17 de novembro, entretanto 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, que deveria ter sido transposta até ao dia até 17 de julho de 2021. Na prática, o regime de acesso aos dados pessoais depende da natureza pública ou privada da entidade que os detém. Por ex., um hospital privado reger-se-á pelo art.º 29.º da LPDP (tratamento de dados de saúde e dados genéticos), ao passo que um hospital E.P.E. reger-se-á pelo art.º 7.º da Lei 26/2016 (acesso e comunicação de dados de saúde), sendo que no setor público, além da figura do encarregado pela proteção de dados existe ainda o responsável pelo acesso aos documentos administrativos (art.º 9.º da 26/2016).

(109) O tratamento de dados pessoais no âmbito de relações laborais, incluindo a utilização de dados biométricos e de meios de vigilância à distância, é regulado nos Art.os 17.º a 21.º do Código do Trabalho, que salvaguarda ainda a confidencialidade de mensagens, nomeadamente de correio eletrónico, e o acesso – designadamente pela *internet* – a informação de caráter não profissional nos termos do art.º 22.º.

(110) Os fins de investigação científica de interesse geral justificam tratamentos de dados nos termos do *RGPD*, *vd.* em especial os Art.os 9.º/2-j), 14.º/5-b), 17.º/3-d, e 21.º/6, e os *considerandos* 26, 33, 50 a 53, 62, 65, 113, 156 e 157, e 160. Sobre a questão vd., Parlamento Europeu, *How the General Data Protection Regulation changes the rules for scientifc research,* EPRS Brussels 2019. Em relação aos dados não pessoais o princípio é que eles devem estar disponíveis gratuitamente em formato legível por máquina e formatos abertos para alimentar o aprendizado de máquina e a IA. Segundo o considerando (9) do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho de 14 novembro de 2018, sobre um quadro para o livre fluxo de dados não pessoais na EU, "A internet das coisas, a inteligência artificial e a aprendizagem automática, que estão em expansão, representam grandes fontes de dados não pessoais, por exemplo, em consequência da sua utilização em processos automatizados de produção industrial. Exemplos concretos de dados não pessoais incluem conjuntos de dados agregados e anonimizados utilizados para a análise de grandes volumes de dados, os dados relativos à agricultura de precisão que podem ajudar a controlar e a otimizar a utilização de pesticidas e de água ou ainda dados sobre as necessidades de manutenção de máquinas industriais. Se os progressos tecnológicos permitirem transformar dados anonimizados em dados pessoais, esses dados devem ser tratados como dados pessoais, e o Regulamento (UE) 2016/679 deve ser aplicado em conformidade." O mesmo princípio se aplica à reutilização de informação do setor público, ao abrigo da Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa a dados abertos e à reutilização de informação do setor público (reformulada). Vd. também Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho, de 30 de maio de 2022, sobre governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Lei sobre Governação de Dados).

público, ou para fins de investigação científica ou histórica ou para fins estatísticos" (Art.º 89.º)[110]. Em especial, podem ser derrogados os direitos de acesso, de retificação, de limitação e de oposição na medida em que esses direitos possam impossibilitar ou prejudicar gravemente a realização dos fins específicos de investigação científica ou histórica ou fins estatísticos, na medida em que tais derrogações sejam necessárias para a prossecução desses fins (Art.º 89.º/2). Por exemplo, a pseudonimização só é obrigatória se os referidos fins puderem ser alcançados desse modo, caso contrário não é obrigatória.

14. Direitos processuais de proteção dos dados pessoais

Os titulares de dados pessoais têm o direito de reclamar junto de uma autoridade de controlo (Art.º 77.º), bem como o direito de agir judicialmente contra uma autoridade de controlo (Art.º 78.º) e/ou contra um responsável pelo tratamento ou um subcontratante (Art.º 79.º). Para o efeito, podem ser representados por organismos sem fins lucrativos (Art.º 35.º LPDP), incluindo associações de defesa dos consumidores[111].

O *RGPD* garante expressamente o direito a obter uma indemnização por danos causados pela violação de dados pessoais (Art.º 82.º). Os titulares dos dados deverão ser *integral e efetivamente* indemnizados pelos danos que tenham sofrido. Como informa o considerando (85), "Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares".

[111] Acórdão de 29 de julho de 2019, C-40/17 – *FashionID*, ECLI:EU:C:2019:629.

Por outro lado, sempre que os responsáveis pelo tratamento ou os subcontratantes estiverem envolvidos no mesmo tratamento, cada um deles deverá ser responsabilizado pela totalidade dos danos causados (responsabilidade solidária). Porém, se os processos forem apensos num único processo judicial, em conformidade com o direito dos Estados-Membros, a indemnização poderá ser repartida em função da responsabilidade que caiba a cada responsável pelo tratamento ou subcontratante pelos danos causados em virtude do tratamento efetuado, na condição de ficar assegurada a indemnização integral e efetiva do titular dos dados pelos danos que tenha sofrido. Qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indemnização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento [Art.º 82.º/4-5 e considerando (146)].

O titular de dados pode intentar uma ação judicial contra o responsável pelo tratamento perante os tribunais do seu Estado-Membro de residência ou os tribunais do Estado-Membro de estabelecimento do responsável pelo tratamento, ressalvando-se, todavia, a *competência exclusiva* destes últimos se o responsável pelo tratamento "for uma autoridade de um Estado-Membro no exercício dos seus poderes públicos" (Art.º 79.º/1-2; vd. Art.º 34.º LPDP).

Para ser exonerado de responsabilidade, o responsável pelo tratamento de dados ou o subcontratante terão que provar que o facto que causou o dano não lhe é de modo algum imputável, nos termos do Art.º 82.º/3 e do considerando (146). No direito interno, estabelece o Art.º 33.º/2 da LPDP que "O responsável pelo tratamento e o subcontratante não incorrem em responsabilidade civil se provarem que o facto que causou o dano não lhes é imputável". Inverte-se, por conseguinte, o ónus da prova, no sentido de ter que ser o responsável pelo tratamento a provar que o facto danoso não lhe é imputável[112].

(112) *Vd.* Mafalda Miranda Barbosa, "Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil", *Revista Bolsa, Banca e Seguros* 3 (2018), p. 215-6, em nota. De notar que o *RGPD* não prejudica a aplicação da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de junho de 2000 relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico»), em matéria nomeadamente de responsabilidade dos prestadores intermediários de serviços previstas nos seus Art.os 12.º a 15.º (art.º 2.º/4), entretanto suprimidos substituídos pelos Art.os 4.º a 6.º e 8.º do Regulamento dos Serviços Digitais: Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE. Sobre este RSD, vd. Luís Manuel de Menezes Leitão, *Digital Services Act (DSA). O regulamento Europeu 2022/2065 sobre os serviços digitais,* Coimbra, Almedina, 2023.

15. Síntese

A proteção dos dados pessoais é cada vez mais importante, em especial no contexto da sociedade da informação, da economia digital e do desenvolvimento da Inteligência Artificial. Derivada da tutela do direito à vida privada e de outros bens da personalidade, a proteção dos dados pessoais corporiza o direito à autodeterminação informativa. O responsável pelo tratamento de dados assume um papel central no regime jurídico dos dados das pessoas humanas, apenas sendo isentas as atividades exclusivamente pessoais ou domésticas (grosso modo, consumidores, incluindo usuários de redes sociais).

De um modo geral, o responsável pelo tratamento deve respeitar os princípios relativos ao tratamento de dados pessoais, assim como os direitos dos titulares, cabendo-lhe ainda cooperar com a autoridade de controlo (CNPD), em especial notificando-a de violação de dados, proceder à avaliação o impacto dos tratamentos e registar tratamento sob sigilo, aplicar medidas técnicas e organizativas adequadas para cumprir o *RGPD*, protegendo os dados desde a conceção e por defeito, em especial através de medidas de segurança informática adequadas ao risco, designar representante quando não estiver estabelecido na UE (salvo para atividades ocasionais e sem tratamento em grande escala de dados sensíveis), e designar encarregado de proteção de dados (EPD/DPO). Além disso, o responsável pelo tratamento pode comprovar a *data compliance* mediante a adoção e implementação de códigos de conduta ou procedimentos de certificação junto de organismos acreditados, incluindo obtenção de selos e marcas de proteção de dados, aprovados pela Comissão Europeia ou CNPD, consoante os casos. Finalmente, o responsável pelo tratamento deve indemnizar integral e efetivamente os titulares de dados pelos danos sofridos (sendo solidária a responsabilidade no caso de tratamento conjunto por vários responsáveis ou subcontratante, sem prejuízo de ação de regresso), e fica sujeito ao pagamento de coimas, que podem chegar a 4% do seu volume de negócios a nível mundial.

Por tudo isto, as empresas e os organismos públicos devem desenvolver as melhores práticas no sentido de prosseguirem uma política responsável em matéria de proteção de dados na qual a pessoa humana não seja reduzida a mero objeto de dados, ou seja, a «datificação reificadora».

5 | DA DISCIPLINA DA SEGURANÇA NA PROTEÇÃO DE DADOS, APLICADA AO PODER LOCAL[103]

*Manuel David Masseno**[104]

1. Um ponto de partida, a segurança dos dados pessoais

Do *Regulamento Geral sobre a Proteção de Dados* da UE – União Europeia, o *RGPD*[105] consta um dever de "segurança no tratamento" para o respetivo responsável e/ou o subcontratante. O qual está, desde logo, subjacente a um dos Princípios relativos ao tratamento de dados pessoais, o da «integridade e confidencialidade», pois os dados devem ser "Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas" (Art.º 5.º n.º 1 f)[106].

---

* Professor auxiliar do Instituto Politécnico de Beja.

(103) Este texto foi sobretudo construído a partir das aulas lecionadas ao *Mestrado em Engenharia Informática* do Instituto Politécnico de Beja, desde 2010, e ao *Curso de Pós-Graduação Avançada em Direito da Proteção de Dados* do Centro de Investigação em Direito Privado da Faculdade de Direito da Universidade de Lisboa, desde 2020.

(104) Professor Adjunto e Encarregado da Proteção de Dados do Instituto Politécnico de Beja. É Membro convidado do PDPC – Centro de estudos e análise da privacidade e proteção de dados da Universidade Europeia, de Lisboa e integra a EDEN – Rede de Especialistas em Proteção de Dados da Europol – a Agência da União Europeia de Cooperação Policial.

(105) Por extenso, Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>, aplicável desde o dia 25 de maio de 2018. Salvo quando expressamente indicado, todos os preceitos referidos são do *RGPD*.

(106) Em atenção aos objetivos do presente trabalho, privilegiaremos ao máximo a transcrição de excertos dos textos originais, sobretudo se de natureza legislativa, relativamente a paráfrases, de modo a facilitar a identificação e o entendimento das Fontes, pois nem é espectável que todos os leitores tenham conhecimentos aprofundados em matéria de Direito da Proteção de Dados. Pelas mesmas razões, abster-me-ei de enquadrar o texto com um aparato doutrinal, apenas indicando no final os Comentários e os Manuais entretanto publicados em Portugal.

O que em especial se concretiza na previsão, em cujos termos, "Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco [...]" (Art.º 32.º n.º 1).

Especificando a regra, segundo a qual, "Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades." (Art.º 24.º n.º 1)[107].

A serem efetivadas "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 [Consequentemente,] o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento *[i.e., by Design* e *by Default]* [...] as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia

(107) O que é explicado no *Considerando* (83) do Regulamento: "A fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a cifragem. Essas medidas deverão assegurar um nível de segurança adequado, nomeadamente a confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função dos riscos e da natureza dos dados pessoais a proteger. Ao avaliar os riscos para a segurança dos dados, deverão ser tidos em conta os riscos apresentados pelo tratamento dos dados pessoais, tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a danos físicos, materiais ou imateriais.".

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 regulamento e proteja os direitos dos titulares dos dados." (Art.º 25.º n.º 1)[108].

Sempre tendo na devida consideração que "Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. [...]" (Art.º 35.º n.º 1), podendo inclusive exigir uma "consulta prévia" à CNPD – Comissão Nacional de Proteção de Dados "[...] quando a avaliação de impacto sobre a proteção de dados [...] indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco." (Art.º 36.º).

Consequentemente, "O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo [Princípio da] («responsabilidade»)." *[proactiva*[109], ou *accountability]* (Art.º 5.º n.º 2).

---

[108] A este propósito, são especialmente de atender *as Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados desde a Conceção e por Defeito* (Versão 2.0), de 20 de outubro de 2020, do CEPD – Comité Europeu para Proteção de Dados <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_pt>.

[109] Como a designa a versão em língua espanhola do *RGPD*, de modo a distingui-la das responsabilidades civil (Art.º 82.º), contraordenacional (Art.º 83.º) e, ainda, penal (Art.º 84.º, esta em termos de abertura aos Estados-membros da UE, a qual foi aproveitada por Portugal com os Art.ºs 46.º a 54.º da Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados <https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982>, habitualmente designada como "Lei de Execução", dando seguimento a uma via aberta pela Lei n.º 3/73, de 5 de abril, aprova várias medidas respeitantes à proteção da intimidade da vida privada <https://diariodarepublica.pt/dr/detalhe/lei/3-1973-675640>, a qual esteve na origem da criminalização da "Devassa por meio da informática" (Art.º 193.º) pelo *Código Penal* de 1985, o qual foi, muito recentemente, revogado e substituído pela "Devassa através de meio de comunicação social, da Internet ou de outros meios de difusão pública generalizada", por força da Lei n.º 26/2023, de 30 de maio <https://diariodarepublica.pt/dr/detalhe/lei/26-2023-213706993>.

2. Uma omissão... voluntária, as regras de segurança

É necessário ter presente que do *RGPD* não consta a previsão de serem aprovadas quaisquer normas de segurança vinculativas, cuja observância seria auditada pelas Autoridades nacionais[110]. Apenas são enunciados padrões genéricos, as, denominadas, "medidas técnicas e organizativas adequadas", a serem determinados em função de critérios casuísticos, resultantes de análises de risco (Art.os 25.º n.os 1 e 2 e 32.º n.º 1), ou, como referimos, estando preenchidos os correspondentes pressupostos de avaliações de impacto (Art.º 35.º).

Com efeito, o Regulamento limita-se enunciar que tais medidas devem "[...] assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado: [...] b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; [dispondo ainda de] d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento." (Art.º 32.º n.º 1).

---

(110) No que se afasta do regime determinado pela Diretiva *ePrivacy* (concretamente, do Art.º 4.º da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, alterada pela Diretiva 2009/136/CE, de 25 de novembro de 2009 <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02002L0058-20091219>, transposta pelo Art.º 3.º da Lei n.º 46/2012, de 29 de agosto, alterando a Lei n.º 41/2004, de 18 de agosto <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2004-106523049>), conforme ao qual a Comissão [Europeia] está habilitada a adotar "normas técnicas de execução"; assim como no que se refere ao Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32014R0910>, o qual atribui-lhe poderes para aprovar normas em múltiplos aspetos dos regimes através de atos de execução e de atos delegados; sem esquecer o Regulamento de Execução (UE) 2018/151 da Comissão, de 30 de janeiro de 2018, que estabelece normas de execução da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho no respeitante à especificação pormenorizada dos elementos a ter em conta pelos prestadores de serviços digitais na gestão dos riscos que se colocam à segurança das redes e dos sistemas de informação, bem como à especificação pormenorizada dos parâmetros para determinar se o impacto de um incidente é substancial <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R0151>.

Aliás, mesmo ao remeter para a adoção de esquemas autorregulatórios, como os códigos de conduta (Art.os 40.º e 41.º)[111] ou a certificação (Art.os 42.º e 43.º)[112], evidenciou também que, se o seu acatamento "[...] pode ser utilizado como elemento para demonstrar o cumprimento das obrigações [...]" (Art.º 32.º n.º 3), o mesmo não exime de eventuais responsabilidades, só as graduando (Art.º 83.º n.º 2 d)), e só no referente à responsabilidade contraordenacional. Embora, o mesmo critério possa também relevar para a determinação judicial das responsabilidades civil e penal, modulando a culpa.

Apenas assim não ocorre, quando, com base numa regra excecional habilitante do Regulamento (Art.º 9.º n.º 4), a nossa *Lei de Execução* determina que "as medidas e os requisitos técnicos mínimos de segurança inerentes ao tratamento de ["dados de saúde" e de "dados genéticos", "categorias especiais de dados", ou dados sensíveis, definidos no Art.º 4.º 15) e 13), respetivamente] são aprovados por portaria dos membros do Governo responsáveis pelas áreas da saúde e da justiça [...]" (Art.º 29.º n.º 7)[113].

---

[111] Sobre a função destes, temos as *Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679* (Versão 2.0), de 4 de junho de 2019, do CEPD <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_pt.pdf>.

[112] A cujo propósito, o CEPD aprovou as *Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento* (Versão 3.0), de 4 de junho de 2019 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf>.

[113] O tratamento destas categorias especiais de dados é também regido pela Lei n.º 12/2005, de 26 de janeiro, sobre informação genética pessoal e informação de saúde <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2005-106603593>, regulamentada pelo Decreto-Lei n.º 131/2014, de 29 de agosto <https://diariodarepublica.pt/dr/detalhe/decreto-lei/131-2014-56384883>, assim como pela Lei n.º 95/2019, de 4 de setembro, a *Lei de Bases da Saúde* <https://diariodarepublica.pt/dr/detalhe/lei/95-2019-124417108>; no entanto, estes diplomas não preveem regras sobre a segurança dos dados e a referida portaria ainda não foi publicada, passados 4 anos sobre a entrada em vigor da *Lei de Execução*.

Embora não sejam os destinatários mais principais desta previsão, os Municípios e as Freguesias, atendendo às respetivas atribuições, estarão também abrangidos por estas regras[114].

2.1. Os referenciais possíveis para uma densificação

Ainda que apenas vinculantes para a Administração direta do Estado, e de um modo reflexo para a indireta, as normas técnicas detalhadas constantes da Resolução do Conselho de Ministros n.º 41/2018, de 28 de março[115], dando andamento à respetiva adequação ao *RGPD*, podem servir como parâmetros. Aliás, os Municípios e as Freguesias deveriam ter recebido estas normas através de atos próprios, ficando alinhadas com o Estado. Pelo menos, sempre que a respetiva escala comporte meios operativos suscetíveis de as implementar efetivamente.

Do mesmo modo, as novas normas técnicas *ISO/IEC 27001:2022* (Sistemas de gestão da segurança da informação) e *ISO/IEC 27002:2022* (Segurança da informação – cibersegurança – privacidade), devidamente complementadas pela norma *ISO/IEC 27701:2019* (Técnicas de segurança – Extensão das normas *ISO/IEC 27001* e da *ISO/IEC 27002* para gestão da proteção de privacidade – orientações e diretrizes)[116], podem desempenhar esse mesmo papel de referência, sobretudo se no âmbito de procedimentos

---

(114) O tratamento destas categorias especiais de dados é também regido pela Lei n.º 12/2005, de 26 de janeiro, tal como pela Lei n.º 26/2016, de 22 de agosto, sobre informação genética pessoal e informação de saúde <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2005-106603593> e <https://diariodarepublica.pt/dr/detalhe/lei/26-2016-75177807>, regulamentada pelo Decreto-Lei n.º 131/2014, de 29 de agosto <https://diariodarepublica.pt/dr/detalhe/decreto-lei/131-2014-56384883>, assim como pela Lei n.º 95/2019, de 4 de setembro, a Lei de Bases da Saúde <https://diariodarepublica.pt/dr/detalhe/lei/95-2019-124417108>; no entanto, estes diplomas não preveem regras sobre a segurança dos dados e a referida portaria ainda não foi publicada, passados 4 anos sobre a entrada em vigor da Lei de Execução.

(115) Com efeito, a Resolução do Conselho de Ministros n.º 41/2018, de 28 de março, define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais <https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/41-2018-114937034>, só é vinculativa para a Administração direta, sendo apenas recomendada para a indireta e para o setor empresarial do Estado.

(116) Para mais informações a propósito destas normas e acesso, pago, às mesmas, vejam-se as seguintes páginas da ISO – a Organização Internacional de Normalização: <https://www.iso.org/standard/27001>, <https://www.iso.org/standard/75652.html> e <https://www.iso.org/standard/71670.html>.

de certificação. Embora, nunca devamos esquecer que o seu exato cumprimento não exime os responsáveis pelo tratamento das respetivas responsabilidades, mormente das de natureza civil ou criminal, a serem sempre determinadas por decisões dos tribunais e não pela CNPD.

Quanto a estas questões, cabe ainda referir a muito recente aprovação, pela CNPD, da Diretriz/2023/1, de 10 de janeiro, sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais. Esta, tem por base a sua atribuição quanto a "Promove[r] a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações nos termos do presente regulamento" (Art.º 57.º n.º 1 d), e na qual a nossa Autoridade enumera um conjunto genérico de boas práticas. No entanto, em linha com o antes explicitado, tais medidas não têm um caráter vinculativo... salvo para a própria CNPD ao avaliar a adequação das ações dos responsáveis pelo tratamento e dos subcontratantes (Art.os 32.º a 34.º e 83.º n.os 2 d) e 4 a), por força do Princípio da boa-fé, ao qual está vinculada enquanto autoridade administrativa independente[117]. Por outras palavras, não de trata de uma "diretriz", em qualquer aceção do termo, nem poderia jamais relevar em atenção ao seu conteúdo, o qual muito pouco ou nada acrescenta ao já previsto pelo *RGPD*.

[117] Nos termos dos Art.os 10.º e 2.º n.º 4 a) do *Código do Procedimento Administrativo*, aprovado pelo Decreto-Lei n.º 4/2015, de 7 de janeiro <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2015-105602322>, aplicável por força do disposto no Art.º 4.º n.º 1 da *Lei de Execução.*

2.2. as normas no domínio da cibersegurança

Por outro lado, embora não devendo ser confundidas com as pertinentes ao nosso objeto, temos as regras aplicáveis à segurança do ciberespaço. Porém, as mesmas, relevando para a segurança dos sistemas informáticos, permitem também limitar os riscos e os danos relativamente aos conteúdos qualificáveis enquanto dados pessoais.

Assim, enquanto não dispusermos de um "sistema europeu de certificação" aplicável[118], relevarão os diversos regimes relativos à aprovação de normas em matéria de cibersegurança, por via legislativa ou regulamentar nacional. Designadamente, o *Regime Jurídico da Segurança no Ciberespaço*[119], transpondo a *Diretiva [NIS]SRI* [1][120], prevê a definição de requisitos de segurança, através de "legislação própria" (Art.º 12.º n.º 1).

No entanto, é necessário ter na devida conta que, "Os requisitos de segurança são definidos de forma a permitir a utilização de normas e especificações técnicas internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação [...]" (Art.º 12.º n.º 3), o que nos remete, implicitamente, para as normas *ISO/IEC* e não para outras, escolhidas arbitrária ou discricionariamente pelo Governo ou pela Administração Pública[121].

---

[118] Conforme ao previsto, sobretudo, nos Art.os 51.º e 52.º do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 *(Regulamento Cibersegurança)* <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32019R0881>.

[119] CLei n.º 46/2018, de 13 de agosto <https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384>.

[120] A Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União < https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016L1148>, a qual deverá ser atualizada até 17 de outubro de 2024, por força do Art.º 41.º n.º 1 da Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva NIS / SRI 2) <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022L2555>.

3. as "medidas técnicas e organizativas adequadas"[122]

Sendo certo que no *RGPD* apenas estão, explicitamente, previstas a "pseudonimização e a cifragem dos dados pessoais" (Art.º 32.º n.º 1 a), cumpre ampliar o nosso campo de análise, sempre sem sair do próprio Regulamento. O que faremos em seguida.

3.1. um critério básico para o tratamento, a "minimização"

Assim e em primeiro lugar, embora tenda a ser pouco referida neste contexto, a minimização está subjacente a toda a disciplina. Inclusive, sendo qualificada como um Princípio, o da «minimização dos dados», os quais devem ser "Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados" (Art.º 5.º n.º 1 c).

O que ocorre também na sua dimensão temporal, ainda que a mesma tenha sido autonomizada no Princípio da «limitação da conservação», devendo ser "Conservados de uma forma que permita a identificação

---

(121) O que não teve as devidas consequências por força da "abertura" constante com o Decreto-Lei n.º 65/2021, de 30 de julho <https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988>, o qual regulamentou o *Regime Jurídico da Segurança do Ciberespaço*, designadamente no que se refere aos conteúdos do *Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança* <https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf>, assim como do QNRCS – *Quadro Nacional de Referência para a Cibersegurança* <https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf>, especificado através do *Quadro de Avaliação de Capacidades de Cibersegurança* <https://www.cncs.gov.pt/docs/cncs-quadrodeavaliacao.pdf>, todos aprovados pelo Centro Nacional de Cibersegurança com base nos poderes regulamentares previsto no Art.º 10.º n.º 10 do antes referido Decreto-Lei, os quais, porventura, estarão mais próximos do *Cybersecurity Framework* do NIST – *National Institute of Standards and Technology*, dos Estados Unidos da América <https://www.nist.gov/cybersecurity>, questões estas sobre as quais não nos teremos por extravasarem manifestamente o nosso objeto, embora não as devêssemos omitir.

(122) A este propósito e apenas enquanto referencial de boas práticas, a ENISA – Agência da União Europeia para a Cibersegurança publicou, logo em dezembro de 2017, um *Handbook on Security of Personal Data Processing* <https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing>; no mesmo e em termos sucintos, ainda que relativamente detalhados, enunciou os principais riscos e medidas a serem efetivadas em cada âmbito das organizações, não distinguindo entre os Setores Público e Privado; entretanto, em início de 2022, a ENISA avançou para uma perspetivação mais transversal das questões e das medidas técnicas e organizativas, em especial no que se refere às PET – Tecnologias de Reforço da Privacidade, com uma publicação sobre *Data Protection Engineering* <https://www.enisa.europa.eu/publications/data-protection-engineering>.

dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados [...]" (Art.º 5.º n.º 1 e)[123].

Aliás, a conexão entre a Segurança e estes Princípios é posta pelo Legislador em termos explícitos, ao preconizar que "[...] 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 [...] destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização." (Art.º 25.º n.º 1)[124].

Regra depois especificada a propósito das várias dimensões antes enunciadas, determinando que "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. Em especial, essas medidas asseguram que, [igualmente] por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares." (Art.º 25.º n.º 2).

Aliás, o mesmo ocorre a propósito das "regras vinculativas aplicáveis às empresas" nas transferências de dados pessoais para países terceiros ou organizações internacionais (Art.º 47.º n.º 2 d) ou do "[...] tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos [...]" (Art.º 89.º n.º 1).

Em qualquer caso, é evidente a redução dos riscos e das correspondentes responsabilidades, incluindo os ligados à Segurança, se estes Princípios forem estritamente observados.

---

(123) Como esclareceu recentemente o TJUE – Tribunal de Justiça da União Europeia, no seu Acórdão de 20 de outubro de 2022, proferido no Processo C-77/21 – Digi <https://curia.europa.eu/juris/liste.jsf?num=C-77/21>.

(124) Como também resulta, explicitamente, do *Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados desde a Conceção e por Defeito*, do CEPD, cit.; tendo também interesse as considerações constantes das *Diretrizes 2/2019 sobre o tratamento de dados pessoais ao abrigo do artigo 6.º, n.º 1, alínea b), do RGPD no contexto da prestação de serviços em linha aos titulares dos dados* (Versão 2.0), de 16 de outubro <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_pt.pdf>, igualmente do CEPD.

3.2. uma medida... arriscada, a "anonimização" [125]

Quanto a esta, o critério é o da não associação, originária ou provocada, a identificadores. Com efeito, cumpre recordar que "[...] é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular" (Art.º 4.º 1)[126].

Porém, o *RGPD* não considera a anonimização como uma medida destinada a garantir a segurança dos dados pessoais, inclusive em termos explícitos. Consequentemente, "[...] Os princípios da proteção de dados [melhor dizendo, o regime jurídico na sua integridade] não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação. *"(Considerando* (26), *in fine)"* [127].

---

[125] Quanto a esta, bem como às PET passíveis de constituir uma alternativa à anonimização, mesmo se menos eficaz, tem um especial interesse o estudo da ENISA sobre *Data Protection Engineering*, antes indicado, assim como o da OCDE – Organização para a Cooperação e Desenvolvimento Económico, já de 2023, sobre *Emerging privacy-enhancing technologies. Current regulatory and policy approaches* <https://www.oecd.org/publications/emerging-privacy-enhancing-technologies-bf121be4-en.htm>.

[126] Incluindo os quase-identificadores e os metadados [isto é, os dados sobre dados], até porque "As pessoas singulares podem ser associadas a identificadores por via eletrónica [e] Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares.", nos termos do *Considerando* (30) do *RGPD* e ficou patente nos fundamentos do Acórdão de 19 de outubro de 2016, Processo C-582/14, *Breyer*, do TJUE <https://curia.europa.eu/juris/liste.jsf?num=C-582/14>.

[127] Enquanto, a Comissão Europeia, nas suas *Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados não pessoais na União Europeia* (COM(2019) 250 final, de 29 de maio), reiterou que "se determinados dados não pessoais puderem ser associados a uma pessoa de qualquer forma, tornando-os direta ou indiretamente identificáveis, devem ser considerados dados pessoais [designadamente] quando a evolução da tecnologia e da análise de dados torna possível a conversão de dados anonimizados em dados pessoais" <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52019DC0250>, dando seguimento ao teor deste *Considerando*.

A este respeito, é ainda mais explícito o Regulamento sobre os dados não pessoais[128], o qual, além de distinguir "dados pessoais" de "dados não pessoais" e de restringir a sua aplicação a estes, incluindo as situações em que ambos "estejam indissociavelmente ligados", reitera a imperatividade dos regimes de proteção dos dados pessoais (Art.os 2.º n.º 2 e 3.º n.º 1). No entanto e simultaneamente, evidencia como "A internet das coisas, a inteligência artificial e a aprendizagem automática, que estão em expansão, representam grandes fontes de dados não pessoais, por exemplo, em consequência da sua utilização em processos automatizados de produção industrial. Exemplos concretos de dados não pessoais incluem conjuntos de dados agregados e anonimizados utilizados para a análise de grandes volumes de dados [e termina concluindo que] Se os progressos tecnológicos permitirem transformar dados anonimizados em dados pessoais, esses dados devem ser tratados como dados pessoais, e o Regulamento (UE) 2016/679 deve ser aplicado em conformidade." (*Considerando* (9).

O que ocorre com a disponibilização, cada vez mais ampla, de ferramentas de IA – Inteligência Artificial agindo sobre megadados *[Big Data]*, como tem sido também mostrado institucionalmente[129], incluindo as ferramentas tecnológicas à disposição de "terceiros", na aceção do Art.º 4.º 10)[130].

---

(128) Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1807>.

(129) Neste sentido, com uma assertividade crescente, foi-se pronunciando o Grupo de Trabalho do Artigo 29.º – GT 29 (Atual CEPD), no *Parecer n.º 7/2003*, de 12 de dezembro, sobre a *reutilização de informações do setor público e a proteção dos dados pessoais – Estabelecer um equilíbrio* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp83_pt.pdf>, seguido do Parecer *n.º 6/2013*, de 5 de junho, *sobre dados abertos e reutilização de informações do setor público (ISP)* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_pt.pdf>, e sobretudo, no *Parecer n.º 5/2014*, de 10 de abril, *sobre as técnicas de anonimização* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf>; mais recentemente, a AEPD – Autoridade Europeia para a Proteção de Dados e a *Agencia Española de Protección de Datos* produziram um documento conjunto sobre os *10 misunderstandings related to anonymisation*, no qual intentam mostrar tanto as vantagens quanto as limitações desta técnica <https://edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en>, estando o mesmo apenas disponível nas línguas inglesa e castelhana.

Assim, sempre que a tecnologia permitir uma identificação, ou reidentificação, ainda que potencial, pois o critério é de ser uma pessoa "identificável" (Art.º 4.º 1), serão de aplicar os regimes constantes do *RGPD* e o "responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo ([conforme ao Princípio da] «responsabilidade»)" (Art.º 5.º n.º 2, retomado no 24.º n.º 1), cabendo-lhe os riscos de desenvolvimento que resultem do tratamento de tais dados.

O que, no mínimo, impõe reavaliações cíclicas dos riscos inerentes a cada procedimento de anonimização, por parte dos responsáveis pelo tratamento, até com sucessivas avaliações de impacto, designadamente quando estiverem em causa "novas tecnologias", em especial as resultantes do desenvolvimento da IA (Art.º 35.º n.º 1).

Por isso mesmo, a nova Diretiva relativa aos dados abertos e à reutilização de informações do setor público[131] procura efetivar a robustez das anonimizações nos seus âmbitos de aplicação, começando por defini-la como "o processo de transformar documentos em documentos anónimos que não digam respeito a uma pessoa singular identificada ou identificável, ou o processo de tornar anónimos os dados pessoais, por forma a que a pessoa em causa não seja ou deixe de ser identificável." (Art.º 2.º 7)[132-133].

---

[130] Ou seja, "a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais"; como resulta também do Acórdão proferido pelo TJUE no Processo T-557/20 – CUR/AEPD, de 26 de abril de 2023 <https://curia.europa.eu/juris/liste.jsf?language=pt&td=ALL&num=T-557/20>.

[131] Por extenso, a 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 <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32019L1024>; para cujo texto final em muito contribuiu o Parecer n.º 5/2018, sobre a proposta de reformulação da Diretiva relativa à reutilização de Informações do Setor Público (ISP), de 10 de julho, da AEPD (Autoridade Europeia para a Proteção de Dados), enfatizando a importância da anonimização neste domínio, o qual só está disponível na íntegra em língua inglesa<https://edps.europa.eu/sites/edp/files/publication/18-07-11_psi_directive_opinion_en.pdf>, embora tenha sido publicada uma síntese em português <https://edps.europa.eu/sites/default/files/publication/18-07-10_psi_directive_opinion_summary_pt.pdf>.

[132] Como enuncia o respetivo *Considerando* (52), "[…] a reutilização de dados pessoais só é admissível se for respeitado o princípio da limitação da finalidade estabelecido no artigo 5.º, n.º 1, alínea b, e no artigo 6.º, do Regulamento (UE) 2016/679 *[o RGPD]*. Por «informações anónimas» entende-se quaisquer

Por sua vez, o novo Regulamento Governação dos Dados reforça o papel da anonimização, sempre a propósito da "reutilização de determinadas categorias de dados protegidos detidos por organismos do setor público", para lá dos abrangidos pela Diretiva (UE) 2019/1024[134]. Para tanto e além de sublinhar os riscos envolvidos[135], prevê que "os organismos

informações que não digam respeito a uma pessoa singular identificada ou identificável, ou que se refiram a dados pessoais tornados anónimos, por forma a que a pessoa em causa não seja ou deixe de ser identificável. A anonimização das informações é uma forma de conciliar o interesse em tornar as informações do setor público tão reutilizáveis quanto possível com as obrigações decorrentes do direito em matéria de proteção de dados, mas acarreta custos. É conveniente considerar esses custos como um dos elementos que contribuem para o cálculo do custo marginal de divulgação, na aceção da presente diretiva".

[133] Esta Diretiva foi transposta pela Lei n.º 68/2021, de 26 de agosto, que também aprovou os princípios gerais em matéria de dados abertos, alterando a Lei n.º 26/2016, de 22 de agosto, a qual foi republicada <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2021-170221049>, também definindo a «anonimização» como "o processo de transformar informações, dados ou documentos, qualquer que seja a sua forma ou formato, de modo a que não possam revelar pessoa singular identificada ou identificável neles referida, ou o processo de tornar anónimos os dados pessoais, por forma a que a pessoa em causa não seja ou deixe de ser identificável" (Art.º 3.º n.º 1 h) e restringindo fortemente a reutilização dos documentos nominativos não anonimizados, além de prever a cobrança de taxas relativas a tais operações (Art.os 19.º n.º 11, 20.º c), 23.º-A n.º 1 e 14.º n.º 1 c).

[134] O Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados) <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022R0868>, no qual a "«Reutilização» [é definida como] a utilização, por pessoas singulares ou coletivas, de dados detidos por organismos do setor público, realizada para fins comerciais ou não comerciais que não correspondem à finalidade inicial da missão de serviço público para a qual os dados foram produzidos, excetuando o intercâmbio de dados entre organismos do setor público exclusivamente no desempenho das suas missões de serviço público." (Art.º 2.º 2)); sendo uma disciplina também resultante do contributo do Parecer conjunto 3/2021 do CEPD e da AEPD sobre a proposta de Regulamento do Parlamento Europeu e do Conselho relativo à governação de dados (Regulamento Governação de Dados), de 11 de março <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_pt>, produzido durante o correspondente processo legislativo.

[135] Assim, os Considerandos (7) e (8) e (9), respetivamente, dão conta que "Existem técnicas que permitem análises em bases de dados que contêm dados pessoais, tais como a anonimização, a privacidade diferencial, a generalização, a supressão e a aleatorização, a utilização de dados sintéticos ou similares e de outros métodos avançados de preservação da privacidade que poderão contribuir para um tratamento de dados mais favorável à privacidade. Os Estados-Membros deverão prestar apoio aos organismos do setor público para que utilizem da melhor forma essas técnicas e, consequentemente, disponibilizem para partilha o máximo possível de dados. [Em qualquer caso,] A reidentificação dos titulares dos dados a partir de conjuntos de dados anonimizados deverá ser proibida. Tal proibição deverá aplicar-se sem prejuízo da possibilidade de realizar investigação sobre técnicas de anonimização, em especial para garantir a segurança da informação, melhorar as técnicas de anonimização existentes e contribuir para a robustez geral da anonimização, em conformidade com o Regulamento (UE) 2016/679".

do setor público asseguram, em conformidade com o direito da União e nacional, que a natureza protegida dos dados seja preservada [para o que,] Podem [melhor dizendo, devem] estabelecer os seguintes requisitos: a) O acesso para fins de reutilização de dados só deve ser concedido se o organismo do setor público ou o organismo competente, na sequência de um pedido de reutilização, tiver assegurado que os dados: i) foram anonimizados, no caso dos dados pessoais" (Art.º 5.º).

Adicionalmente, "[…] O organismo do setor público reserva-se o direito de verificar o processo, os meios e quaisquer resultados do tratamento de dados efetuado pelo reutilizador para preservar a integridade da proteção dos dados e reserva-se o direito de proibir a utilização de resultados que contenham informações que comprometam os direitos e interesses de terceiros. […]" e "[…] Os reutilizadores ficam proibidos de reidentificar qualquer titular dos dados a quem os dados digam respeito e devem tomar medidas técnicas e operacionais para prevenir a reidentificação e para notificar ao organismo do setor público qualquer violação de dados que resulte na reidentificação dos titulares dos dados em causa. […]" (Art.º 5.º n.os 4 e 5).

Para terminar, cumpre não esquecer que a própria anonimização é uma das "operações tratamento", sendo apenas lícita se estiver presente algum dos fundamentos previstos e for realizada através das "[…] medidas técnicas adequadas […] destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento […]", no contexto da proteção de dados desde a conceção, incluindo avaliações de impacto prévias, sempre que necessário (Art.os 4.º 2), 6.º, 9.º, 25.º n.º 1 e 35.º n.º 1 do *RGPD, designadamente*).

(136) A propósito da operacionalização desta, ainda que centrado num dos setores no qual é mais comum, até necessariamente, o da saúde, a ENISA publicou o estudo *Deploying Pseudonymisation Techniques*, em março de 2022 <https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques>

(137) Assim, nos *Considerandos* (28), (29), (75), (78), (85) ou (156), designadamente nos dois primeiros temos que "A aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento e os seus subcontratantes a cumprir as suas obrigações de proteção de dados. A introdução explícita da «pseudonimização» no presente regulamento não se destina a excluir eventuais outras medidas de proteção de dados." e "A fim de criar incentivos para aplicar a pseudonimização durante o tratamento de dados pessoais, deverá ser possível tomar medidas de pseudonimização, permitindo-se simultaneamente uma análise geral, no âmbito do mesmo responsável pelo tratamento quando este tiver tomado as medidas técnicas e organizativas necessárias para assegurar, relativamente ao tratamento em questão, a aplicação do presente regulamento e a conservação em separado das informações adicionais que permitem atribuir os dados pessoais a um titular de dados específico. O responsável pelo tratamento que tratar os dados pessoais deverá indicar as pessoas autorizadas no âmbito do mesmo responsável pelo tratamento".

(138) Aliás, estas limitações da pseudonimização já constavam, amplamente, do *Parecer* n.º 5/2014, do GT 29, *sobre as técnicas de anonimização*, antes referido.

139) Especificamente, ao alertar para o facto de "[…] Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. [e] Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. […]", tal como enuncia o *Considerando* (26).

(140) Neste caso e como resulta do *RGPD*, "O tratamento […] está sujeito a garantias adequadas, nos termos do presente regulamento, para os direitos e liberdades do titular dos dados. Essas garantias asseguram a adoção de medidas técnicas e organizativas a fim de assegurar, nomeadamente, o respeito do princípio da minimização dos dados. Essas medidas podem incluir a pseudonimização, desde que os fins visados possam ser atingidos desse modo. Sempre que esses fins possam ser atingidos por novos tratamentos que não permitam, ou já não permitam, a identificação dos titulares dos dados, os referidos fins são atingidos desse modo." (Art.º 89.º n.º 1).

3.3. uma medida menos eficaz, a "pseudonimização" [136]

Neste caso, temos uma definição normativa, consistindo no: "[...] tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;" (Art.º 4.º 5).

E, além de ser, reiteradamente, sugerida pelo Regulamento em sede de Considerandos[137] e surgir qualificada como constituindo uma "[...] medida técnica adequada para assegurar um nível de segurança adequado ao risco [...]" (Art.º 32.º n.º 1 a), constitui "o exemplo" de entre as "[...] medidas técnicas [...] adequadas [...] destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento [...]", no contexto da proteção de dados desde a conceção (Art.º 25.º n.º 1), sendo ainda a sua especificação remetida para os "códigos de conduta" (Art.º 40.º n.º 2 d).

Mas, "o problema" está em a reidentificação dos titulares dos dados ser ainda mais fácil tecnicamente que com a anonimização. Neste caso, a mesma poderá resultar não só com base nas analíticas de *Big Data*, mas também por outras vias, como as correlações internas aos registos, a notícias de jornal, ao acesso a dados de tráfego ou a registos de operações de cartões de crédito, bem como pela reversão dos pseudónimos através de força bruta computacional, com ou sem a utilização de ferramentas de IA[138].

Daí, a preocupação manifesta do Legislador com os riscos inerentes à "inversão não autorizada da pseudonimização"[139]. O que exige, ou torna muito aconselhável, uma pseudonimização forte, incluindo a dos quase-identificadores, já próxima das técnicas de cifragem.

Porém, a pseudonimização pode constituir a única medida técnica disponível, sobretudo quando for inviável a anonimização dos dados, como ocorre com os arquivos, uma realidade de especial relevância para as Autarquias Locais[140]. O mesmo ocorre quanto à "reutilização

de determinadas categorias de dados protegidos detidos por organismos do setor público", no Regulamento Governação dos Dados, o qual admite também o recurso à pseudonimização[141], embora com cautelas[142].

Por último, como clarificou o Tribunal de Justiça[143], é preciso acentuar que os dados não são univocamente anonimizados ou pseudonimizados, dependendo sempre das informações licitamente à disposição do responsável pelo tratamento ou de um terceiro. O mesmo podendo afirmar-se a propósito do subcontratante.

3.4. a saída que ficou por assumir, a "cifragem" [144]

Antes de mais, cabe acentuar como esta só é referida pelo Regulamento, sem sequer a definir e sempre a par da pseudonimização, a propósito dos tratamentos que não tenham por base o consentimento dos titulares

---

[141] Especificamente, no Considerando (15) é explicitado que "[...] Nos casos em que o fornecimento de dados anonimizados ou alterados não responda às necessidades do reutilizador, sob reserva de terem sido cumpridos todos os requisitos para a realização de uma avaliação de impacto em matéria de proteção de dados e a consulta da autoridade de controlo, nos termos dos artigos 35.º e 36.º do Regulamento (UE) 2016/679 [o *RGPD*], e os riscos para os direitos e interesses dos titulares dos dados tenham sido considerados mínimos, poderá ser permitida a reutilização dos dados [mas, apenas] nas instalações ou de forma remota num ambiente de tratamento seguro. Tal poderá consistir num mecanismo adequado para a reutilização de dados pseudonimizados. As análises de dados realizadas nesses ambientes de tratamento seguros deverão ser supervisionadas pelo organismo do setor público, a fim de proteger os direitos e interesses de terceiros. [...]".

[142] Efetivamente e ainda nos termos do Considerando (15), "[...] Em especial, os dados pessoais só deverão ser transmitidos a terceiros para reutilização se existir uma base jurídica ao abrigo do direito de proteção de dados que permita essa transmissão. Os dados não pessoais só deverão ser transmitidos se não houver motivos para crer que a combinação de conjuntos de dados não pessoais conduziria à identificação dos titulares dos dados. O mesmo se deverá aplicar aos dados pseudonimizados que mantêm o seu estatuto de dados pessoais. Em caso de reidentificação dos titulares dos dados, a obrigação de notificar essa violação de dados ao organismo do setor público deverá aplicar-se, para além da obrigação de notificar essa violação de dados a uma autoridade de controlo e ao titular dos dados em conformidade com o Regulamento (UE) 2016/679. [...]".

[143] No recentíssimo Acórdão CUR/AEPD, o qual levou até ao limite as considerações já constantes do Acórdão Breyer, ambos já referidos.

[144] Sobre esta e logo em novembro de 2013, durante o processo legislativo conducente à adoção do *RGPD,* a ENISA publicou um estudo sobre as *Recommended cryptographic measures – Securing personal data* <https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data>, enquanto os desafios de médio prazo são enfrentados no *Post-Quantum Cryptography: Current state and quantum mitigation <https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation?v2=1>*, de maio de 2021, depois complementado pelo *Post-Quantum Cryptography – Integration study* <https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study?v2=1>, de outubro de 2022.

dos dados ou disposições de natureza legislativa limitadoras dos seus direitos e liberdades fundamentais (Art.º 6.º n.º 4 e) e da segurança no tratamento (Art.º 32.º n.º 1 a).

Aliás, por si só, apenas surge a propósito da isenção de responsabilidades no caso de ocorrerem incidentes de segurança, sempre que "O responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem." (Art.º 34.º n.º 3 a).

Embora, devamos acentuar o facto de a "cifragem dos dados pessoais" (Art.º 32.º n.º 1 a), só por si, não ser bastante para afastar as responsabilidades no respeitante às consequências de incidentes de segurança, por apenas garantir a confidencialidade dos dados, não as respetivas integridade e disponibilidade, nomeadamente quando a cifragem resulta de uma ação maliciosa de terceiros, como nos ataques de *ransomware,* ou os dados forem apagados ou ficarem inacessíveis devido a algum caso fortuito.

Daí, o caráter cumulativo das medidas de segurança previstas, i.e., "A capacidade de assegurar [não só] a confidencialidade, [mas também a] integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;", "A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico", e, ainda, a implementação de "Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento." (Art.º 32.º n.º 1, b), c) e d).

Ainda assim, a cifragem é aconselhável perante grandes riscos, designadamente perante o "Tratamento de categorias especiais de dados pessoais" (Art.º 9.º), mormente se for identificada como uma medida apropriada na sequência de avaliações de impacto (Art.º 35.º).

Porém, é necessário ter presente as distintas perspetivas das Instituições e das agências da União Europeia perante a cifragem, sobretudo se forte, pelas suas implicações em termos de segurança e de combate à criminalidade organizada e ao terrorismo[145].

Embora, em coerência com a Cultura da UE, os processos legislativos têm resultado em compromissos, como mostram o *Código Europeu das Comunicações Eletrónicas*[146], e a *Diretiva [NIS/] SRI 2*, enquanto exemplos recentes.

---

[145] Em termos muito sintéticos, podemos salientar como o PE – Parlamento Europeu, o CEPD, a AEPD, a FRA – Agência Europeia para os Direitos Fundamentais e ainda a ENISA – Agência da União Europeia para a Cibersegurança a defendem, desde logo, com a *Resolução sobre a luta contra a cibercriminalidade,* do PE, de 3 de outubro de 2017 (2017/2068(INI) <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52017IP0366>, seguida pela *Declaração sobre a cifragem e o seu impacto na proteção dos indivíduos relativamente ao tratamento dos seus dados pessoais na UE,* ainda do GT 29, de 11 de abril de 2018 <https://ec.europa.eu/newsroom/article29/items/622229/en>, os Relatórios sobre Direitos Fundamentais, da FRA, sobretudo de 2017 e de 2018 <http://fra.europa.eu/pt>, *o Parecer sobre Cifragem – Uma cifragem forte garante a nossa identidade digital,* da ENISA, de dezembro de 2016 <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption>, e a *Declaração Conjunta sobre uma investigação criminal lícita que respeite a proteção dos dados no século XXI,* da Europol – Agência de Polícia da União Europeia e da ENISA, de 20 de maio de 2016, apesar das reservas da Europol<https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection>; no outro polo tem estado o Conselho, com a maioria dos Estados-Membros, e também a Europol, concretizadas na Resolução do Conselho sobre a *Encriptação – Segurança através da encriptação e segurança apesar da encriptação,* de 24 de novembro de 2020 <https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/pt/pdf>, e, com um ênfase crescente, nas IOCTA – Avaliações sobre o Crime Organizado na Internet da Europol, desde 2016 <https://www.europol.europa.eu/publications-events/main-reports/iocta-report>; enquanto a Comissão tem tido uma posição ambivalente, embora pendendo para a do Conselho, como mostram a Proposta de Regulamento relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas – *ePrivacy*), (COM(2017) 10 final), de 10 de janeiro de 2017 <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52017PC0010>, a Comunicação Conjunta da Comissão e da Alta Representante da União para os Negócios Estrangeiros e Política de Segurança – *Resiliência, dissuasão e defesa: reforçar a cibersegurança* na UE (JOIN(2017) 450 final), de 13 de setembro de 2017 <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52017JC0450>, e a Comunicação sobre a Estratégia da UE para a União da Segurança (COM(2020) 605 final), de 24 de julho de 2020 <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52020DC0605>, ou ainda a Comunicação Conjunta da Comissão e do Alto Representante da União para os Negócios Estrangeiros e Política de Segurança – *Estratégia de Cibersegurança da UE para a Década Digital* (JOIN(2020) 18 final), de 16 de dezembro de 2020 <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52020JC0018>.

[146] Estabelecido pela Diretiva (UE) 2018/1972, de 11 de dezembro de 2018 <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018L1972>, como resulta do respetivo Art.º 40.º n.º 1 e, sobretudo, dos *Considerandos* (96) e (97), a qual foi transposta pela Lei n.º 16/2022, de 16 de agosto, que aprova a *Lei das Comunicações Eletrónicas,* transpondo as Diretivas 98/84/CE, 2002/77/CE e (UE) 2018/1972, alterando as Leis n.os 41/2004, de 18 de agosto e 99/2009, de 4 de setembro, e os Decretos-Leis n.os 151-A/2000, de 20 de julho, e 24/2014, de 14 de fevereiro, e revogando a Lei n.º 5/2004, de 10 de fevereiro, e a Portaria n.º 791/98, de 22 de setembro <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2022-187527517>, relevando para o efeito o disposto no Art.º 59.º n.º 1.

Em Portugal, esta questão estará *resolvida pela Carta Portuguesa de Direitos Humanos na Era Digital*[147], em cujos termos, "Todos têm direito a comunicar eletronicamente usando a criptografia e outras formas de proteção da identidade ou que evitem a recolha de dados pessoais, designadamente para exercer liberdades civis e políticas sem censura ou discriminação." (Art.º 8.º n.º 1). Embora se trate de um direito dos titulares dos dados, no mínimo estará presente um dever de não interferência por parte dos responsáveis pelo tratamento, senão mesmo de predisporem os meios técnicos necessários para o efetivar.

Além de o *Código Europeu das Comunicações Eletrónicas* e a nova *Lei das Comunicações Eletrónicas*[148], que o transpôs, terem alargado o respetivo âmbito aos serviços OTT *(Over-the-top)* de comunicação bidirecional, isto é, às mensagens de texto e de voz e às chamadas de voz e de vídeo, designadamente no âmbito de redes sociais[149], mesmo que não impliquem a atribuição pública de números conforme aos planos de numeração nacionais e internacional, como exigia a legislação anterior.

---

[147] Aprovada pela Lei n.º 27/2021, de 17 de maio <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2021-164870244>.

[148] Especificamente, o Art.º 2.º 5) do *Código* define como "«Serviço de comunicações interpessoais», o serviço oferecido, em geral mediante remuneração, que permite o intercâmbio interpessoal direto e interativo de informações através de redes de comunicações eletrónicas entre um número finito de pessoas, através do qual as pessoas que participam ou dão início à comunicação determinam o(s) seu(s) destinatário(s) e não inclui serviços que permitem a comunicação interpessoal e interativa que funcionem de modo acessório e que estejam intrinsecamente ligados a outro serviço", assim explicitando o seu âmbito de aplicação, enunciado no Art.º 1.º n.º 1, enquanto a nossa Lei o faz nos Art.os 1.º e 3.º n.º 1 tt), igualmente a propósito do «Serviço de comunicações interpessoais».

[149] Como explica o Considerando (15) do *Código Europeu das Comunicações Eletrónicas,* "Os serviços utilizados para fins de comunicações, e os meios técnicos usados para prestar esses serviços, evoluíram consideravelmente. Os utilizadores finais trocam cada vez mais a tradicional telefonia vocal, as mensagens de texto (SMS) e os serviços de envio de correio eletrónico por serviços em linha equivalentes em termos de funcionamento, tais como os serviços de voz em IP (VoIP), os serviços de mensagens e os serviços de correio eletrónico baseados na Web (webmail). Para garantir que os utilizadores finais e os seus direitos são eficazmente protegidos e beneficiam da mesma proteção quando utilizam serviços funcionalmente equivalentes, a definição, orientada para o futuro, do conceito de «serviços de comunicações eletrónicas» não deverá basear-se meramente em parâmetros técnicos, mas antes numa abordagem funcional. O âmbito da regulação necessária deverá ser adequado aos seus objetivos de interesse público. Embora o «envio de sinais» continue a ser um importante parâmetro para determinar os serviços abrangidos pelo âmbito de aplicação da presente diretiva, a definição deverá abranger também os outros serviços que permitem a comunicação. Do ponto de vista do utilizador final é irrelevante se é o fornecedor a enviar ele próprio os sinais ou se a comunicação é efetuada através de um serviço de acesso à Internet, [...]".

4. Quando a segurança falha, a "violação de dados pessoais" (150)

Antes de tudo o mais, é indispensável evidenciar como, no âmbito do género "incidentes de segurança", o Regulamento ocupa-se apenas de uma espécie, a "«Violação de dados pessoais»: [a qual consiste em] uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (Art.º 4.º 12)(151).

Ora, esta não deve ser confundida, de todo, com a "violação dos direitos" dos titulares dos dados (Art.º 79.º n.º 1) ou com a "violação do [presente] regulamento" (Art.os 77.º n.º 1, 79.º n.º 1, 82.º n.º 1, 83.º ou 84.º), isto é, com quaisquer falhas, no que respeita à sua responsabilidade "proativa", por parte do responsável pelo tratamento dos dados(152).

Aliás, como enunciou repetidamente o CEPD, as situações de destruição, de dano, de perda ou de tratamento não autorizado ou ilícito podem ser enquadradas numa tipologia, consistente na "violação de

---

(150) Sobre estas questões, é indispensável levar em consideração o disposto nas *Guidelines 9/2022 on personal data breach notification under GDPR* (Versão 2.0), de 28 de março de 2023 [ainda sem uma versão em língua portuguesa]<https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_pt>, que sucederam ao Parecer 03/2014, de 25 de março, *relativo à notificação da violação de dados pessoais* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_pt.pdf>, e às *Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679*, de 3 de outubro de 2017 / 6 de fevereiro de 2018 <https://ec.europa.eu/newsroom/article29/items/612052/en> ambos ainda do GT 29; entretanto, esclarecidas pelas *Orientações sobre exemplos da notificação de uma violação de dados pessoais* (Versão 2.0), adotadas em 14 de dezembro de 2021 <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_pt>, estas já do CEPD.

(151) Porque, "Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo [!?] ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares. [...]", como conta do *Considerando* (85).

(152) Como ficou demonstrado pelo teor da Deliberação/2021/1569, de 21 de dezembro, da CNPD, a propósito de múltiplos incumprimentos do *RGPD* por parte do Município de Lisboa, entre os quais não esteve a falta de notificação do ocorrido à Comissão, porque não ocorreu qualquer "violação de dados pessoais", contrariamente ao que muitos "comentadores" se apressaram a dizer à Comunicação Social <https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121953>.

confidencialidade", na "violação de integridade" ou na "violação de disponibilidade" dos dados, sempre pressupondo atos maliciosos ou casos fortuitos, tanto de origem externa quanto interna.

Cumpre ainda acrescentar, quanto aos atos maliciosos, inclusive praticados por terceiros, que estaremos ainda perante um tratamento de dados, em sentido próprio, isto é, "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (Art.º 4.º 2), cuja ilicitude não afasta a aplicação dos princípios e regras constantes do Regulamento. Incorrendo os seus autores nas inerentes responsabilidades, incluindo a responsabilidade civil (Art.º 82.º) e a contraordenacional (Art.º 83.º)[153], pois são qualificáveis como "responsáveis pelo tratamento", por "determina[rem] as finalidades e os meios de tratamento de dados pessoais" (Art.º 4.º 7).

4.1. o procedimento interno

Em todos os casos, o "responsável pelo tratamento documenta quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à autoridade de controlo verificar o cumprimento do disposto no presente artigo." (Art.º 33.º n.º 5)[154].

---

[153] Além da responsabilidade penal resultante do, eventual, preenchimento das previsões típicas correspondentes aos crimes de "Acesso indevido" (Art.º 47.º), de "Desvio de dados" (Art.º 48.º), de "Viciação ou destruição de dados" (Art.º 49.º) e ou de "Inserção de dados falsos" (Art.º 50.º), todos da *Lei de Execução*.

[154] O que não corresponde apenas a uma especificação do dever geral de registo de todas as operações de tratamento, Art.º 30.º e é explicado pelo Considerando (82), "A fim de comprovar a observância do presente regulamento, o responsável pelo tratamento ou o subcontratante deverá conservar registos de atividades de tratamento sob a sua responsabilidade. Os responsáveis pelo tratamento e subcontratantes deverão ser obrigados a cooperar com a autoridade de controlo e a facultar-lhe esses registos, a pedido, para fiscalização dessas operações de tratamento.", pois as operações de tratamento em causa, incluindo "[...] a limitação, o apagamento ou a destruição;" (Art.º 4.º 2)), podem ser imputáveis a terceiros.

Do mesmo modo, o responsável pelo tratamento, ou o subcontratante, deve adotar medidas para reparar os efeitos da violação de dados e "[...] inclusive, se for caso disso [...] para atenuar os seus eventuais efeitos negativos" (Art.º 33.º n.º 3 d).

O que supõe uma análise dos riscos para "[...] os direitos e liberdades das pessoas singulares. [...]" (Art.º 33.º n.º 1), de modo a poder determinar, e se necessário demonstrar, a desnecessidade de notificar a violação de dados à CNPD, quando os mesmos forem nulos ou extremamente reduzidos[155].

Na análise em questão, deve ser imediatamente envolvido o Encarregado da Proteção de Dados (Art.os 38.º n.º 1 e 39.º n.º 1 a) e b) do *RGPD* e Art.º 11.º b) da Lei de Execução), o qual terá "[...] em devida consideração os riscos associados [...]" (Art.º 39.º n.º 2), desde uma posição de autonomia técnica reforçada (Art.os 38.º n.º 3 do *RGPD* e 9.º n.º 2 da Lei de Execução) e atendendo à previsão consistente em ser o "Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento [...]" (Art.º 39.º n.º 1 e)[156-157].

---

[155] Como enuncia o Considerando (75), ainda que em termos gerais e prévios a qualquer "violação de dados pessoais", "O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados."; consequentemente, "A probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento de dados. Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado", conforme ao Considerando (76).

Para a mesma, podem servir de referência os critérios de exclusão da comunicação ao titular dos dados (Art.º 34.º n.º 3 a) e b), com as devidas adaptações resultantes dos graus de risco, além de não ultrapassar o prazo de notificação à Autoridade, salvo se justificadamente (Art.º 33.º n.º 1). Contudo, esta análise não deve ser confundida com uma avaliação de impacto sobre a proteção de dados, inclusive atendendo ao momento, aos pressupostos e aos critérios previstos para a mesma (Art.º 35.º)[158].

4.2. a notificação à CNPD e a comunicação aos titulares dos dados

No entanto, se da violação de dados pessoais for suscetível de resultar num risco [mesmo pequeno] para os direitos e liberdades das pessoas singulares, "[...] o responsável pelo tratamento notifica desse facto a autoridade de controlo competente [...], sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma [...]" (Art.º 33.º n.º 1). No caso de a mesma ter sido identificada por um subcontratante, este deve notificar, melhor dizendo informar, o responsável pelo tratamento, "[...] sem demora injustificada após ter conhecimento [...]" da mesma (Art.º 33.º n.º 2), ao caber apenas a este a análise dos riscos envolvidos e a correspondente obrigação de notificar a CNPD.

---

[156] Neste sentido, de um modo explícito, embora sem a aprofundar a questão, as *Orientações sobre os encarregados da proteção de dados (EPD)*, de 13 de dezembro de 2016, com revisão e última redação adotada em 5 de abril de 2017, do GT 29 <https://ec.europa.eu/newsroom/article29/items/612048>.

[157] Embora a tal não estejam obrigados, será também aconselhável estabelecer um diálogo a este respeito com o responsável de segurança, obrigatoriamente nomeado por todas as Autarquias Locais, nos termos e para os efeitos previstos no Art.º 5.º do Decreto-Lei n.º 65/2021, de 30 de julho, independentemente de se verificarem os pressupostos constantes do Art.º 15.º do *Regime Jurídico da Segurança do Ciberespaço* e explicitados nos Art.os 11.º a 17.º do Decreto-Lei antes referido.

[158] A este propósito, o *Considerando* (84) enuncia que "A fim de promover o cumprimento do presente regulamento nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco. Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento. [...]"; sendo também de sublinhar a relevância das *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679*, de 4 de abril de 2017, revistas e adotadas pela última vez em 4 de outubro de 2017, ainda do GT 29 <https://ec.europa.eu/newsroom/article29/items/611236/en>.

Da notificação devem constar, "pelo menos [uma descrição da] natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa [,bem como,] o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações [uma descrição das] consequências prováveis da violação de dados pessoais [e outra das] medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos;" (Art.º 33.º n.º 3). Podendo a mesma ser faseada, quando tal seja justificável, objetivamente (Art.º 33.º n.º 4).

Por seu turno, se "[...] a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada." (Art.º 34.º n.º 1), por iniciativa própria ou por exigência da CNPD (Art.º 34.º n.º 4).

Todavia, esta comunicação não é exigida ao responsável pelo tratamento, inclusivamente pelos altos custos reputacionais eventualmente envolvidos ou para evitar uma perceção de insegurança pública excessiva, se este "[...] tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem;" ou "[...] tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados [...] já não é suscetível de se concretizar." (Art.º 34.º n.º 3 a) e b).

Distinta e eventualmente mais gravosa para o responsável pelo tratamento é a decorrente da desproporcionalidade, ou da inviabilidade material, de comunicar a violação a todos os titulares dos dados cujos direitos e liberdades tenham ficado em risco com a violação, caso em que "[...] é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz." (Art.º 34.º n.º 3 c).

4.3. as outras comunicações legalmente devidas

No que se refere às violações de dados pessoais em sistemas informáticos no Poder Local, à notificação à CNPD junta-se o dever de o fazer ao "Centro Nacional de Cibersegurança [quanto aos] incidentes com um impacto relevante na segurança das redes e dos sistemas de informação [...]" (Art.º 15.º n.º 1 do *Regime Jurídico da Segurança do Ciberespaço)*. Os pressupostos e os procedimentos desta notificação, constantes deste preceito, são depois detalhados no Decreto-Lei n.º 65/2021[159].

Consequentemente, de acordo com a *Diretiva [NIS/] SRI*[160] e com o *Regime Jurídico da Segurança do Ciberespaço* (Art.os 12.º e 13.º), estamos perante uma duplicação de deveres de notificar.

Daí também a previsão legal de uma cooperação, ou pelo menos de um diálogo, entre as respetivas autoridades, no nosso caso, entre o Centro Nacional de Cibersegurança e a CNPD, designadamente reportando entre si os incidentes de segurança dos quais tiverem conhecimento. Embora não esteja legalmente previsto qualquer alinhamento regulatório ou de procedimentos[161], até em atenção ao Primado do *RGPD*

---

[159] Especificamente, nos Art.os 11.º a 16.º, relevando também e em especial o *Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança* e o *Quadro de Avaliação de Capacidades de Cibersegurança,* já referidos, bem como e ainda, o Regulamento n.º 183/2022, de 21 de fevereiro, do Centro Nacional de Cibersegurança, o qual aprovou a *Instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes* <https://www.cncs.gov.pt/docs/regulamento-183-2022.pdf>.

[160] Nos Art.os 2.º n.º 1 e 15.º n.º 4, tal como clarifica o *Considerando* (63), "Os dados pessoais ficam em muitos casos comprometidos em consequência de incidentes. Neste contexto, as autoridades competentes e as autoridades encarregadas da proteção dos dados deverão cooperar e trocar informações sobre todas as questões pertinentes para combater as eventuais violações de dados pessoais resultantes de incidentes.".

[161] Explicitando o Art.º 3.º n.os 3 a) e c) do Decreto-Lei n.º 65/2021 que "O cumprimento dos requisitos de segurança e das obrigações de notificação de incidentes previstos no Regime Jurídico da Segurança do Ciberespaço e no presente decreto-lei não prejudica: a) O cumprimento dos requisitos específicos de segurança e das obrigações específicas de notificação de incidentes nos termos definidos pelas autoridades competentes, nomeadamente [...] pela Comissão Nacional de Proteção de Dados (CNPD) [...]", não estando esta entre "As entidades referidas no n.º 1 do artigo anterior [as quais] podem estabelecer formas de colaboração com vista ao cumprimento das obrigações em matéria de requisitos de segurança e de notificação de incidentes previstos no Regime Jurídico da Segurança do Ciberespaço, e no presente decreto-lei, numa lógica de partilha de recursos, desde que seja assegurada a efetiva operacionalização das mesmas em cada entidade", o que é confirmado pelo disposto no Art.º 2.º n.º 7 do Decreto-Lei em cujos termos "O disposto na presente lei não prejudica o cumprimento da legislação aplicável em matéria: a) De proteção de dados pessoais, designadamente o disposto no Regulamento (UE) n.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados)".

e à independência garantida por este a cada Autoridade competente (Art.os 51.º a 58.º)[162].

Por último, não deve ser esquecido o dever de denunciar ao Ministério Público os "[...] crimes de que tomarem conhecimento no exercício das suas funções e por causa delas;" que incumbe aos funcionários das Autarquias Locais[163], designadamente dos previstos e punidos pela *Lei de Execução*.

[162] E assim continuará com a *Diretiva [NIS/] SRI 2*, a partir de 18 de outubro de 2024, como prevê o respetivo Art.º 31.º n.º 2, "Quando tratarem de incidentes que tenham originado violações de dados pessoais, as autoridades competentes devem trabalhar em estreita cooperação com as autoridades de supervisão nos termos do Regulamento (UE) 2016/679, sem prejuízo das competências e funções que incumbem às autoridades de supervisão nos termos desse regulamento", porque, como explica *Considerando* (108), "Os dados pessoais ficam amiúde expostos em consequência de incidentes. Nesse contexto, as entidades competentes deverão cooperar e trocar informações sobre todas as questões pertinentes com as autoridades referidas no Regulamento (UE) 2016/679 [...]".

[163] Por força do previsto no Art.º 242.º n.º 1 b) do *Código do Processo Penal*, aprovado pelo Decreto-Lei n.º 78/87, de 17 de fevereiro <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1987-34570075>.

Referências

PINHEIRO, Alexandre Sousa (Coord.). *Comentário ao Regulamento Geral sobre Proteção de Dados.* Coimbra: Almedina, 2018, sobretudo pp. 448-457, da autoria de Alexandre Sousa Pinheiro e de Carlos Jorge Gonçalves.

CORDEIRO, A. Barreto Menezes (Coord.). *Comentário ao Regulamento Geral sobre Proteção de Dados e à Lei n.º 58/2019*. Coimbra: Almedina, 2021, sobretudo pp. 266-279, da autoria de Francisco Rodrigues Rocha.

CORDEIRO, A. Barreto Menezes. *Direito da Proteção de Dados – À luz do RGPD e da Lei n.º 58/2019*. Coimbra: Almedina, 2020, sobretudo pp. 346-352.

MONIZ, Graça Canto. *Manual de Introdução à Proteção de Dados Pessoais*. Coimbra: Almedina, 2023, sobretudo pp. 241-258.**I.**

6 | A ADMINISTRAÇÃO LOCAL E AS REDES SOCIAIS

CML / Equipa de Projeto de Proteção de Dados Pessoais*

Resumo

O presente artigo foca-se na relação da administração pública local com a Internet, concretamente no que concerne à divulgação de imagem e som nas redes sociais. Isto é, temos como intuito a análise da possibilidade de recurso às redes sociais dos órgãos das autarquias locais para divulgação de conteúdos com dados pessoais. Deste modo, este artigo estrutura-se em quatro domínios: (I) Princípios da Administração Pública – revela-se necessário, numa fase inicial, abordar a matéria de acesso à informação administrativa para melhor entender-se a importância deste direito na Administração Pública, vertido tanto no princípio da publicidade como no princípio da transparência. De seguida, desenvolve-se a correlação do princípio da administração aberta e acesso à informação com o princípio da proteção dos dados pessoais; (II) Relação entre o *RGPD* e a publicação de dados pessoais na *Internet* e nas redes sociais pelos órgãos das autarquias locais – procede-se ao estudo das regras aplicáveis à publicação de imagem e/ou voz na *Internet* e nas redes sociais pelos órgãos das autarquias locais e a aplicação do *RGPD* nestes contextos, nomeadamente a integração de preceitos como dados pessoais, tratamento de dados e fundamento de licitude; (III) Uso das redes sociais pelos órgãos das autarquias locais – analisa-se as práticas de publicação de imagem e /ou voz na Internet e nas redes sociais dos órgãos das autarquias locais, bem como as suas vantagens e desvantagens. Além disso, são estudadas as consequências do uso das redes sociais, nomeadamente quanto à relação das empresas de redes sociais com as autarquias locais, o tratamento de dados transfronteiriço e internacional. É feita também uma análise especial quanto ao fenómeno da reutilização dos dados pessoais; (IV) Medidas necessárias – onde consta uma reflexão sobre as medidas e as boas práticas a implementar quando estamos perante a publicação de dados pessoais na *Internet* e nas redes sociais, através da sua disponibilização nas redes sociais dos órgãos das autarquias locais. Por último, tecem-se algumas considerações finais procedendo-se a um resumo breve de todo o caminho percorrido ao longo da nossa exposição.

Palavras-chave: Autarquias locais; redes sociais, dados pessoais; transferência internacional de dados pessoais; reutilização; medidas técnicas e organizativas.

---

* Jorge Gomes da Silva, Maria Helena Silva, Maria de Medeiros e Telma Vitória

Introdução

Neste artigo refletimos se, e em que condições, as redes sociais podem ser utilizadas pelos órgãos das autarquias locais como meio de concretização do direito de acesso à informação administrativa, tendo presente os princípios da administração aberta e da proteção de dados pessoais.

Partindo deste pórtico, e conscientes das dificuldades associadas à implementação do Regulamento Geral de Proteção de Dados (*RGPD*), das diferentes interpretações por parte das entidades públicas, das distintas aplicações do princípio da proporcionalidade, na sua relação com os princípios gerais da proteção de dados pessoais e da administração aberta, avançamos com os seguintes objetivos:

- O primeiro objetivo visa refletir sobre a publicação de imagem (de fotografias e vídeos) e da voz (de áudios e/ou vídeos) nas redes sociais da autarquia local, nomeadamente em plataformas como o *Facebook*, *Youtube* e *Instagram*.
- O segundo objetivo comporta uma dimensão prática, baseada na aplicação das normas do *RGPD* ao caso concreto da publicação de dados pessoais nas redes sociais.
- O terceiro objetivo visa a partilha de orientações técnicas e organizativas (boas práticas), de forma a contribuir para a melhoria da conformidade com o *RGPD*.

I. PRINCÍPIOS DA ADMINISTRAÇÃO PÚBLICA

1. A administração aberta e o acesso à informação

Os princípios devem ser encarados como verdadeiras linhas orientadoras com aplicabilidade obrigatória, sendo essenciais na efetiva concretização do Direito num Estado Democrático. Assim sendo, devem revelar-se instrumentos que permitam legitimar a atuação do Direito, bem como limitar qualquer intervenção contrária aos valores democráticos. No âmbito da Administração Pública, o princípio da administração aberta e o princípio do acesso à informação, considerado também como direito, ganham destaque na análise a que nos propomos.

No âmbito do Direito da União Europeia é de referir o Art.º 11.º da Carta dos Direitos Fundamentais da União Europeia (Carta) relativo à liberdade de expressão que integra em si a liberdade de informação tanto para a receber como para a transmitir. Para além disso, entende-se, a partir da leitura do Art.º 42.º da Carta, que os cidadãos da União têm "[...] direito de acesso aos documentos das instituições, órgãos e organismos da União, seja qual for o suporte desses documentos.". Acresce o facto de, já no Art.º 41.º da Carta, quando consagrado o direito a uma boa administração se admitir "[...] O direito de qualquer pessoa a ter acesso aos processos que se lhe refiram [...]"[(164)].

Passando para o âmbito nacional, poderemos notar que neste está refletido o ideal europeu de que uma administração aberta garante o princípio da transparência e da publicidade. Na Constituição da República Portuguesa (CRP) o direito à informação extrai-se do Art.º 37.º com a epígrafe intitulada de "liberdade de expressão e de informação", afirmando que todos os cidadãos têm o direito "[...] de informar, de se informar e de ser informados [...]"[(165)].

---

(164) Cf. alínea b) do n.º 2 do Art.º 41.º da Carta.

(165) Cf. n.º 1 do Art.º 37.º da CRP.

Por sua vez, no Art.º 268.º da CRP encontra-se consagrado o direito de acesso à informação administrativa, sendo que no seu n.º 1 compreende-se que os cidadãos poderão requerer informações sobre o "[...] andamento dos processos em que sejam diretamente interessados [...]"[166], assim como têm o direito de "[...] conhecer as resoluções definitivas [...]"[167] que foram tomadas a seu respeito. Ainda, no mesmo artigo, no seu n.º 2 é referido que os cidadãos têm o direito de aceder a arquivos e registos administrativos, salvaguardando-se o "[...] disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal e à intimidade das pessoas.".

É de referir que o princípio da publicidade, elencado no n.º 1 do Art.º 116.º da CRP, no âmbito dos órgãos colegiais do tipo de assembleia, pressupõe a possibilidade jurídica de livre acesso das pessoas e órgãos de comunicação à sala de sessões, proibição de reuniões secretas e exigência de publicação das atas dos respetivos trabalhos[168]. Para além disso, constitui o princípio democrático de fiscalização popular dos atos públicos e do direito à informação.

Quando falamos em Administração Pública não podemos desmarcar-nos do conceito de interesse público que, embora vasto e de difícil definição, deve ser também o guia orientador da atuação do Estado. Esta íntima relação está refletida no n.º 1 do Art.º 266.º da CRP, que ressalva a importância do respeito pelos cidadãos e pelos seus direitos. Por outro lado, a atuação da Administração Pública não deverá afastar a aplicabilidade dos princípios da igualdade, da proporcionalidade, da justiça, da imparcialidade e da boa-fé como se subentende do n.º 2 do mesmo artigo.

No que concerne à legislação administrativa é de referir que no Art.º 17.º do Código do Procedimento Administrativo (CPA) se encontra consagrado o princípio da administração aberta que ressalva o direito de acesso aos

[166] Cf. n.º 1 do Art.º 268.º da CRP.

[167] Cf. última parte do n.º 1 do Art.º 268.º da CRP.

[168] CANOTILHO, Gomes; MOREIRA, Vital – Constituição da República Portuguesa Anotada, p. 113.

arquivos e registos administrativos, ainda que a pessoa que os pretenda consultar e aceder não esteja diretamente ligada ao procedimento em causa. Se observarmos o Art.º 14.º do CPA que destaca os *"Princípios aplicáveis à administração eletrónica"* torna-se percetível a necessidade de promover uma administração aberta através do uso de meios eletrónicos, "[...] de modo a promover a eficiência e a transparência administrativas e a proximidade com os interessados.".

Em suma, através das normas indicadas poderemos notar que existe a permanente preocupação por parte do legislador em manter a publicidade e a transparência salvaguardadas na atuação da Administração Pública, garantindo que o direito à informação seja concretizado para todos os cidadãos. Só desta forma é possível compreender a Administração Pública como uma verdadeira administração aberta.

2. A articulação com o *RGPD*: princípio da proteção de dados pessoais

É certo que, como tivemos oportunidade de desenvolver, o princípio da administração aberta pressupõe o direito de acesso à informação administrativa. No entanto, a prática deste direito tem de ser feita em correlação com a reserva da vida privada e a proteção de dados pessoais. Nenhum destes direitos tem um alcance ilimitado[169].

Ora, a Carta dos Direitos Fundamentais da União Europeia reconhece o respeito pela vida privada e a proteção dos dados pessoais como direitos fundamentais nos Art.º 7.º e 8.º.

Por outro lado, a CRP, já na sua versão de 1976, consagrava o direito à reserva sobre a intimidade da vida privada. Na versão atual, este direito está presente no Art.º 26.º, que inclui também o direito à imagem e à palavra. Por sua vez, no Art.º 35.º são referidos vários direitos do cidadão relativos à proteção de dados, como o acesso aos dados que lhe digam respeito, a sua retificação, atualização, o direito de conhecer a finalidade a que se destinam, entre outros.

[169] DIAS, José – Direito à Informação, Protecção da Intimidade e Autoridades Administrativas Independentes, p. 17.

No próprio CPA são encontrados vários preceitos referentes à proteção de dados. Tendo como exemplo, no Art.º 17.º do CPA encontra-se estipulado que o princípio da administração aberta se aplica "[...] sem prejuízo do disposto na lei em matérias relativas [...] à privacidade das pessoas.". Para além disso, no Art.º 18.º está consagrado o direito do titular à proteção dos seus dados pessoais.

Destacamos do mesmo modo, o Art.º 83.º onde é referido que o direito ao acesso a documentos por interessados "[...] abrange os documentos relativos a terceiros, sem prejuízo da proteção dos dados pessoais [...]"[170]. Daqui poderemos concluir que, no princípio da administração aberta está incluído o próprio direito à proteção de dados pessoais[171], nomeadamente o Regulamento Geral sobre a Proteção de Dados (*RGPD*[172].

Se assim o aferirmos, poderemos afirmar que o princípio da proteção de dados pessoais não deverá ser (tão só) interpretado como limite na atuação transparente da administração pública, mas antes como garantia e consequência necessária da atuação dessa administração. Nesta linha de raciocínio, a proteção de dados pessoais funcionará como pressuposto do princípio da administração aberta[173].

Do mesmo modo, o direito à proteção de dados pessoais não é um direito absoluto e, como tal, poderá sofrer restrições. No *considerando* (4) do *RGPD* é referido que, este direito deve "[...] ser equilibrado com outros direitos lidade. [...]". Mais se acrescenta, no *considerando* (154), que o direito da União

---

(170) No entanto, deste 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. Acórdão do Supremo Tribunal Administrativo (STA) de 20.12.2017, processo n.º 0870/17. Consultado em http://www.dgsi.pt/jsta.nsf/35fbbbf22e1bb1e680256f8e003ea931/9c55aff4669f54d38025820c005b160e?OpenDocument&ExpandSection=1&Highlight=0,Uni%C3%A3o,Europeia, a 17.06.2021.

(171) MAGALHÃES, Filipa – O Princípio da Administração Aberta e o direito à proteção de dados pessoais: direitos conflituantes ou um direito duplamente garantístico?, p. 97.

(172) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Revogou a Diretiva 95/46/CE. Este Regulamento introduziu um reforço dos direitos dos titulares dos dados e permitiu alertar para a obrigatoriedade de estabelecer regras para o efetivo cumprimento dos direitos, princípios e demais normas sobre proteção de dados.

(173) MAGALHÃES, Filipa – O Princípio da Administração Aberta e o direito à proteção de dados pessoais: direitos conflituantes ou um direito duplamente garantístico?, p. 98.

ou de cada Estado-Membro deve procurar "[...] conciliar o acesso do público aos documentos oficiais e a reutilização da informação do setor público com o direito à proteção dos dados pessoais [...]".

Embora o *RGPD* procure dar ênfase à proteção das pessoas singulares, no que concerne ao respeito pelo tratamento dos seus dados e à livre circulação dos mesmos, como mencionámos, o certo é que o mesmo diploma admite, no Art.º 85.º, a conciliação dessa proteção com a liberdade de informação, atribuindo a cada Estado-Membro o exercício dessa conciliação[174] destes direitos, quando consagra o tratamento e acesso do público aos documentos oficiais.

Face ao exposto, a articulação entre o direito à informação e o direito à proteção de dados pessoais de um determinado titular deve ser feita através de um processo de ponderação ao caso concreto[175]. Como o próprio *RGPD* indica, é perentório a aplicação do princípio da proporcionalidade, explanado também no Art.º 18.º da CRP e no Art.º 7.º do CPA, sendo o "barómetro" que auxilia a decisão de prevalência de um direito em detrimento do outro. Nesse sentido, a ponderação deverá, de igual forma, observar os corolários do princípio da proporcionalidade – o princípio da adequação, da necessidade e da proporcionalidade em sentido estrito[176]. Na atuação administrativa terá de existir uma proporção adequada entre os meios empregues e o fim que se pretende atingir[177]. É de extrema importância que a cedência de informação não revele um sacrifício excessivo e desnecessário.

---

(174) Conforme refere Filipa Matias Magalhães "este é um caso interessante em como a soma de dois direitos essenciais faz surgir um direito duplamente garantístico" – *O Princípio da Administração Aberta e o direito à proteção de dados pessoais: direitos conflituantes ou um direito duplamente garantístico?*, p. 99.

(175) Por exemplo, em certos casos será passível o acesso a determinados dados pessoais, mas essa permissão não poderá deixar de ser articulada com o princípio da minimização dos dados – cf. Art.º 5.º, n.º1 alínea b) do *RGPD* - que limita a própria quantidade de informação tratada.

(176) DIAS, José – Direito à Informação, Protecção da Intimidade e Autoridades Administrativas Independentes, p. 18.

(177) BOTELHO, José – Código do Procedimento Administrativo anotado e comentado, p. 67.

II. RELAÇÃO ENTRE O *RGPD* E A PUBLICAÇÃO DE DADOS PESSOAIS NA *INTERNET* E NAS REDES SOCIAIS PELOS ORGÃOS DAS AUTARQUIAS LOCAIS

Os órgãos das autarquias locais têm como prática a publicação de imagens e vídeos (de eventos, programas, reuniões públicas, entre outros...) no seu sítio *web* institucional e nas suas respetivas redes sociais.

Uma utilização responsável deste tipo de plataformas em linha, requer o conhecimento de todos os efeitos da mesma, nomeadamente o facto do responsável pelo tratamento dos dados pessoais e do titular dos dados em causa perderem o controlo sobre esses mesmos dados pessoais.

1. O tratamento de dados pessoais: imagem e voz

De modo a justificar a aplicação do *RGPD*, nesta secção, a publicação de conteúdos nas redes sociais é inserida nas definições de "dados pessoais" e "tratamento de dados pessoais".

Em primeiro lugar, importa destacar que a imagem (de fotografias e vídeos) e a voz (de áudios e/ou vídeos) de um determinado titular constituem dados pessoais na aceção do Art.º 4.º 1) do *RGPD*, tratando-se de informação relativa a uma pessoa singular identificada ou identificável. Em segundo lugar, na publicação de áudios, vídeos e imagens nas redes sociais e na *Internet* estão subentendidas várias operações de tratamento de dados (descritas no Art.º 4.º 2) do *RGPD*), de entre outras, como a recolha, a organização, a conservação e a própria divulgação[178].

Para além disso, é de referir que a imagem e a voz constituem uma possibilidade de revelar informações que estão inseridas nas categorias especiais de dados pessoais, referidas no Art.º 9.º do *RGPD*. Neste artigo está elencado um grupo de dados que, pela sua natureza, especialmente sensível do ponto vista dos direitos e liberdades fundamentais e dado o contexto dades fundamentais, merecendo, deste modo, uma proteção específica[179].

---

[178] CO termo «divulgação» é definido no Art.º 4.º 2) como transmissão (por exemplo, comunicação individual), difusão (por exemplo, publicação em linha) ou qualquer outra forma de disponibilização.

[179] *Considerando* (51) do *RGPD*.

Isto é, o tratamento destes dados pessoais poderá assumir características que estão incluídas neste grupo de dados (origem racial ou étnica, convicção religiosa, entre outros). Para além disso, é de referir que a voz é considerada um dado biométrico na aceção do Art.º 9.º, n.º 1 do *RGPD*[180], que permite a identificação única de uma determinada pessoa[181].

De notar que o tratamento de dados pessoais de categorias especiais, é em princípio, proibido, havendo, no entanto, exceções elencadas no Art.º 9.º, n.º 2 do *RGPD*.

2. Fundamento de licitude: o consentimento

No que diz respeito ao fundamento de licitude quanto à partilha de dados pessoais na *Internet* e nas redes sociais, não havendo uma norma legal relativa à permissão deste tipo de tratamento de dados, o consentimento prévio e expresso de todas as pessoas abrangidas pela gravação e publicação de imagem e voz nas redes sociais, nos termos da alínea a) do n.º 2 do Art.º 9.º do *RGPD*, deverá ser considerado o único fundamento de licitude daquele tratamento.

De acordo com o *RGPD*, este consentimento tem de ser uma manifestação de vontade livre, específica, informada e inequívoca. O pedido de consentimento deve ser apresentado de modo inteligível, de fácil acesso e numa linguagem clara e simples, não sendo admitidos consentimentos tácitos nem opções pré-validadas. O silêncio, a omissão ou a mera participação no evento não pode ser encarado como um ato positivo inequívoco[182]. Não basta o mero aviso de que os participantes podem solicitar a não recolha da sua imagem.

Para além disso, quanto ao consentimento nas categorias especiais de dados (Art.º 9.º, n.º 2, alínea a) do *RGPD*), é necessário ter em conta que, para além de ter de ser uma manifestação de vontade livre, específica,

---

[180] GT 29 - Parecer 4/2007 sobre o conceito de dados pessoais, p. 9

[181] Art.º 4.º 14) do *RGPD*

[182] MONIZ, Graça – Manual de Introdução à Proteção de Dados Pessoais, p. 80.

informada e inequívoca, o titular deve exteriorizá-lo de forma clara e o mesmo deve ser explícito. O termo explícito é entendido como sinónimo de expresso, excluindo consentimentos indeferidos a partir de condutas ou comportamentos dos titulares[183]. Por exemplo, para garantir que o consentimento é explícito, deverá ser exigida uma assinatura do titular dos dados.

De notar que, o direito à informação, consagrado no Art.º 13.º do *RGPD*, deverá ser efetivado no momento da recolha do consentimento junto do titular. O ato de informar o titular consubstancia-se numa obrigação do responsável pelo tratamento, devendo este dar conhecimento ao titular sobre a finalidade do respetivo tratamento. Para além disto, é importante que o titular dos dados esteja informado sobre o facto das imagens e do som, uma vez disponibilizados em linha, serem suscetíveis de reutilização e difusão por terceiros.

É necessário ter consciência que o titular se poderá opor a esse tratamento, não sendo possível adquirir o seu consentimento. Deste modo, nas situações em que o cidadão se recusa a dar o seu consentimento, para ser fotografado ou recusa a publicação da sua imagem ou voz nas redes sociais e na *Internet,* é obrigatório que o responsável pelo tratamento respeite a sua vontade. Acresce o facto de a recusa do consentimento não poder implicar o não exercício de direitos pelo titular dos dados. A título exemplificativo, um cidadão continua a ter o direito de participar em iniciativas ou eventos realizados por uma Câmara Municipal ou por uma Assembleia Municipal, ainda que não tenha dado permissão para ser fotografado ou filmado. Deste modo, terá o responsável pelo tratamento de tomar as medidas necessárias para que este titular não seja excluído, permitindo proteger os seus dados pessoais, assegurando ao mesmo tempo a sua participação.

[183] MONIZ, Graça – Manual de Introdução à Proteção de Dados Pessoais, p. 80.

Observa-se, perante a leitura do *considerando* (43) do *RGPD*, que "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 [...]". No entanto, como já afirmado pela Autoridade Europeia de Proteção de Dados (AEPD), a utilização deste fundamento de licitude pelas autoridades públicas "[...] não se encontra totalmente excluída do quadro jurídico do *RGPD*.[...]", sendo importante que não exista "[...] qualquer risco de fraude, intimidação, coação ou consequências negativas importantes se o consentimento for recusado [...]"[184].

2.1 Autarquias locais: regras aplicáveis sobre a publicidade das reuniões

No âmbito da publicação da *Orientação relativa à transmissão na Internet das reuniões de órgãos autárquicos* (doravante Orientação)[185] da Comissão Nacional de Proteção de Dados (CNPD), é reservado um espaço neste artigo sobre as conclusões da CNPD sobre esta matéria.

Em primeiro lugar, é de referir que os órgãos autárquicos são obrigados, por lei, a proceder a reuniões de natureza pública, tendo os cidadãos oportunidade de assistir e participar nas mesmas[186].

---

[184] CEPD, Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679, parágrafos 17 e 24. MONIZ, Graça – Manual de Introdução à Proteção de Dados Pessoais, p.73 - 74.

[185] Orientação da Comissão Nacional de Proteção de Dados (CNPD) de 18 de abril de 2023.

[186] A CRP estabelece no n.º 1 do seu Art.º 116.º que "as reuniões das assembleias que funcionem como órgãos de soberania, das regiões autónomas ou do poder local são públicas, exceto nos casos previstos na lei.". Para além disso, o n.º 1 do Art.º 27.º do CPA refere que "as reuniões dos órgãos da Administração Pública não são públicas, salvo disposição legal em contrário.". Esta disposição em contrário encontra-se no n.º 2 do Art.º 49.º do RJAL que prevê igualmente um período para intervenção e esclarecimento do público nas sessões das reuniões públicas mensais dos órgãos executivos das autarquias locais.

Atualmente é usual efetuarem-se gravações e transmissões das sessões dos órgãos autárquicos[187], tendo em conta o caráter público das sessões dos órgãos deliberativos, sendo permitido a qualquer cidadão assistir às mesmas e assim favorecer o conhecimento das políticas e realidades locais. Estas sessões poderão ser consultadas em variados sítios *web* institucionais de órgãos autárquicos, materializando assim, os princípios aplicáveis à administração eletrónica presentes no Art.º 14.º do CPA.

Na Orientação, a CNPD começa por indicar o interesse público na divulgação das reuniões de natureza pública dos órgãos municipais, ressalvando, no entanto, que os cidadãos que participam nestas reuniões têm direito à reserva da vida privada. Deste modo, é defendido que, não existindo uma norma legal que preveja este tratamento de dados nem atribua às autarquias locais uma função de divulgação mediática, o consentimento prévio e expresso de todas as pessoas abrangidas pela gravação e transmissão (incluindo a mera presença de trabalhadores), seria o único fundamento[188] de licitude daquele tratamento[189].

---

[187] De destacar que esta prática se tornou cada vez mais usual aquando da pandemia Covid-19, em que foi concedida a possibilidade de recurso a meios tecnológicos para a realização de reuniões e consequente transmissão. A título de exemplo, podemos referir o Art.º 3.º da Lei n.º 1-A/2020, de 19 de março, na redação dada pela Lei n.º 91/2021 de 17 de dezembro, em que foi estabelecido que, até 30 de junho de 2022, poderia proceder-se à transmissão em direto pela Internet ou outro canal de comunicação das reuniões dos órgãos das autarquias locais de realização pública obrigatória, garantindo assim a transparência e a publicidade. Esta norma foi revogada pela Lei n.º 31/2023 de 4 de julho, pese embora este procedimento se tenha tornado uma prática contínua e intrinsecamente assumida.

[188] A CNPD já teria referido este fundamento de licitude no PARECER/2019/10 sobre o projeto de "Regulamento de transmissão áudio/vídeo em direto e online das reuniões dos órgãos do Município do Cartaxo", adicionando que "[...] o referido consentimento deve ser recolhido não apenas em relação àqueles que, no exercício de funções ou no exercício do direito de participação, façam declarações durante as reuniões, como também em relação aos que exercem o mesmo direito de participação através da mera presença ou assistência naquelas.".

[189] Ainda, nas Orientações, a CNPD salvaguarda, por sua vez que, o tratamento destes dados não poderia ser feito por base no Art.º 9.º, n.º 2, alínea e) – se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular – por ser feito num contexto de exercício de direitos de cidadania.

De igual modo, na Audição Parlamentar sobre a transmissão e divulgação das sessões e reuniões públicas das autarquias locais[190] a Presidente da CNPD Paula Meira Lourenço, a 30 de maio de 2023, reforçou a necessidade de um formulário de consentimento. Aquando das reuniões públicas com transmissão e gravação de imagem e áudio, os titulares de dados devem tomar conhecimento de todas as informações necessárias para que possam fornecer o seu consentimento, se assim o entenderem, concretizando o consagrado no *RGPD*. Relativamente aos cidadãos que se recusem a ser filmados, a Presidente da CNPD deixou orientações claras da necessidade de se proteger o respetivo titular, permitindo que o mesmo exerça o seu direito de participação democrática acautelando a proteção dos seus dados pessoais.

Neste contexto, a CNPD recomenda que a dita transmissão ocorra apenas no sítio da Internet da entidade pública, respeitando os princípios da proporcionalidade e da minimização dos dados e salvaguardando ao mesmo tempo o princípio da administração aberta.

III. USO DAS REDES SOCIAIS PELOS ORGÃOS DAS AUTARQUIAS LOCAIS

Importa notar que, houve um crescente interesse de divulgação de conteúdos, como imagem e voz, que contêm dados pessoais, nas redes sociais dos órgãos das autarquias locais, em parte devido ao avanço do mundo digital e do novo paradigma de comunicação através destes meios tecnológicos. Acresce o facto de assistirmos a uma participação mais ativa dos cidadãos e ao seu interesse em primar pela transparência da própria Administração Pública, exigindo informações sobre o seu modo de atuação, o que em si se revela um ponto muito positivo.

Na perspetiva da verificação do princípio da transparência, o uso das redes sociais é um recurso útil, uma vez que permite chegar a um maior número de pessoas, particularmente aos mais jovens, fomentando assim a participação e informação da autarquia local.

---

[190] ARTV – Audição da Comissão Nacional de Proteção de Dados. [Em linha]. 30 de maio de 2023. Disponível em <URL: https://canal.parlamento.pt/?cid=7083&title=audicao-da-comissao-nacional-de-protecao-de--dados-cnpd>. Consulta em 11 de setembro de 2023.

A utilização da tecnologia dá-nos a oportunidade de ultrapassar barreiras físicas e mobilizar cidadãos, ao convidá-los a participar e a assistir a ações em linha, concretizando a verdadeira Democracia e promovendo a eficácia e a participação cívica. Ao mesmo tempo, permite reduzir custos de comunicação contribuindo para a ligação dos cidadãos aos candidatos. Ora, é inegável que as redes sociais são uma privilegiada fonte de informação, para os cidadãos avaliarem as forças políticas locais e decidirem o seu voto de forma mais informada.

No entanto, existem sempre riscos perante o uso de plataformas em linha, pela própria natureza do mundo digital onde todos os conteúdos podem ser recuperáveis e atravessam fronteiras que vão para além do controlo do responsável pelo tratamento e do domínio dos titulares dos dados pessoais. Se anteriormente nos referimos ao princípio da proporcionalidade como "balança" de ponderação em caso de conflito de direitos, é essencial a sua aplicação quanto à utilização da *Internet* e das redes sociais para divulgação de informações. Iremos desenvolver estas consequências nas seguintes secções.

1. Posição das redes sociais em relação às autarquias locais

As plataformas como o *Youtube, Instagram* e *Facebook* são considerados plataformas em linha de grande dimensão[191], pois têm um número médio mensal de destinatários ativos do serviço, na União Europeia, igual ou superior a 45 milhões, tendo "[...] um alcance maior e um maior impacto na influência sobre a forma como os destinatários do serviço obtêm informações e comunicam em linha, [...]"[192].

Aquando da publicação de dados pessoais numa rede social, o responsável pelo tratamento tem de ter em conta de que está a enviá-los para uma plataforma que não está sob seu controlo e que por isso deve ter uma política de proteção de dados diferente, que afeta não só os titulares dos dados pessoais que são publicados, mas até os próprios visitantes

[191] De acordo com o Art.º 33.º, n.º 1 do Regulamento dos Serviços Digitais (Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho).

[192] *Considerando* (57) do Regulamento dos Serviços Digitais (DSA).

da página. A título de exemplo, refere-se o resultado da AIPD feita pelo Ministério do Interior Holandês à utilização de páginas de *Facebook* por parte do Governo[193]. De entre as conclusões, destaca-se o facto de o *Facebook* considerar-se um responsável pelo tratamento independente para todos os dados pessoais que recolhe sobre os visitantes de uma página governamental, podendo assim tratar esses dados pessoais para os seus próprios fins. De acordo com esta AIPD, as organizações governamentais têm de considerar o *Facebook* como uma empresa comercial terceira à qual divulgam todos os dados pessoais dos visitantes da sua página, visto que não existe um contrato sobre o tratamento de dados subjacente, a utilização de uma página resulta na divulgação de dados de terceiros. Deste modo, é indicado que não há necessidade de as organizações governamentais divulgarem dados pessoais desta forma. De facto, o *Facebook* não informa claramente o que faz com os dados e como determina quais as publicações que os visitantes veem no seu *feed* de notícias.

É necessário ter em conta que, no que toca à publicação nas redes sociais, as autarquias locais e a empresa detentora da rede social não poderão ser consideradas responsáveis conjuntos pelo tratamento, na aceção do Art.º 26.º do *RGPD*, pois a empresa detentora da rede social é a única que determina as finalidades e os meios desse tratamento[194].

Do mesmo modo chama-se à atenção para as situações em que é necessária a autenticação prévia antes da prestação de serviço ou informação. Por vezes, para esta autenticação é feito o recurso a empresas terceiras cuja área de negócio é o tratamento de dados pessoais em larga escala. Por exemplo, para aceder a uma determinada conta no sítio *web* de uma autarquia local, o utilizador poderá fazer a autenticação através da sua conta do *Facebook, Google* ou *Eventbrite*. Nestas situações, o pedido de autorização é feito pelo prestador dos serviços de autenticação sem

---

[193] Embora, esta AIPD não seja focada na publicação de fotos e vídeos de cidadãos nas redes sociais, continua a ser pertinente na medida em que refere os perigos da simples criação de página de *Facebook* por uma entidade governamental e nas consequências para os dados pessoais dos visitantes. Privacy Company, "DPIA on government *Facebook* Pages".

[194] Esta afirmação vai encontro da decisão do ACÓRDÃO DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, FASHION ID, C-40/17, EU:C:2019:629 (2019-07-29).

que, previamente, o utilizador seja notificado de que os seus dados irão passar a ser tratados por uma entidade diferente da inicial e sem que lhe seja pedido consentimento para esse fim.

Nestes casos, o responsável pelo tratamento tem de avaliar a necessidade da autenticação prévia e, se este método for imprescindível, deve recorrer a meios próprios (registo na plataforma) ou disponibilizar meios alternativos nacionais tais como a autenticação através do Cartão de Cidadão, chave móvel digital ou do Portal das Finanças. O recurso a prestadores externos, designadamente, as empresas que disponibilizam plataformas em linha de grande dimensão, deve ser evitada. Caso, se possibilite a autenticação, o acesso e/ou a navegação através daquelas entidades, deve ser dada, obrigatoriamente, a respetiva informação relativa ao tratamento de dados pessoais realizado pelas entidades terceiras, bem como deve ser obtida, por ato inequívoco, a respetiva tomada de conhecimento (consciencialização) por parte do titular dos dados.

2. Publicação nas redes sociais como transferência de dados pessoais para um país terceiro ou organização internacional

Como já foi referido, o responsável pelo tratamento de dados, terá de ter em conta as consequências da publicação de dados pessoais numa plataforma em linha, nomeadamente, as políticas de privacidade da própria plataforma e a sua possível transferência de dados para outro país fora da União Europeia[195].

Ora, a publicação de dados pessoais em redes sociais comporta um tratamento transfronteiriço (entre Estados-Membros)[196] e até internacional (fora da União Europeia)[197] na aceção do *RGPD*. Só o facto de o

---

[195] De acordo com o Art.º 44.º do *RGPD*, *"qualquer transferência de dados pessoais que seja ou venha a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento [...)]"*. Isto é, uma transferência de dados para país terceiro só poderá ser lícita se tiver por base uma decisão de adequação (Art.º 45.º), tiver sido sujeita a garantias adequadas designadamente regras vinculativas aplicáveis às empresas (Art.º 47.º), ou se preencher as condições do Art.º 49.º do *RGPD*.

[196] Art.º 4.º 23) do *RGPD*.

[197] Art.º 44.º *RGPD*.

armazenamento dos dados poder ser feito pela empresa detentora da rede social fora da União Europeia e, de utilizadores de todo o mundo poderem consultar esses dados, já demonstra que este tratamento inclui fluxos internacionais de dados pessoais suscetíveis de pôr em risco os direitos e liberdades de pessoas singulares.

Como exemplo, chamamos à atenção para os acórdãos do Tribunal de Justiça da União Europeia (TJUE) Schrems I[198] e Schrems II[199], que surgiram no âmbito de um litígio com Max Schrems, ativista da privacidade, sobre transferência de dados pessoais de utilizadores da rede social *Facebook* para os Estados Unidos. Estes acórdãos invalidaram a Decisão «Porto Seguro» (Decisão 2000/520/CE, de 26 de julho de 2000) e a Decisão «Escudo de Privacidade» (Decisão de Execução (UE) 2016/1250, de 12 de julho de 2016), que serviram como base para as transferências de dados da UE para os EUA, por não garantirem um nível de proteção adequado[200].

A síntese destes casos serve para demonstrar que, a transferência de dados pessoais para entidades externas (como redes sociais que são habitualmente utilizadas por milhares de utilizadores) que, por sua vez, transferem para países terceiros, comportam riscos elevados para os seus titulares.

Deste modo, é reforçada novamente a necessidade de os titulares terem de ser informados de que as autarquias locais têm a intenção de divulgar os seus dados pessoais numa plataforma em linha, cuja política de privacidade não é por elas controlada, tendo os titulares o direito de consentir ou recusar esta publicação.

---

(198) ACÓRDÃO DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Schrems, C-362/14, EU:C:2015:650 (2015-10-06).

(199) ACÓRDÃO DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Facebook Ireland e Schrems, C-311/18, EU:C:2020:559 (2020-07-16).

(200) Atualmente, uma das bases de transferência de dados da UE para os EUA é a decisão de adequação Quadro de Privacidade dos Dados UE-EUA, adotada pela Comissão Europeia no dia 10 de julho de 2023. Comissão Europeia, *Commercial sector: adequacy decision on the EU-US Data Privacy Framework*. Max Schrems, por sua vez, defende que a nova decisão de adequação não assegura aos cidadãos europeus um nível de proteção adequado dos seus dados pessoais, tendo já anunciado que pretende levar a nova decisão ao TJUE. *European Commission gives EU-US data transfers third round at CJEU (noyb.eu).*

3. Reutilização dos dados pessoais

Nesta secção, consideramos pertinente desenvolver de forma sucinta o significado do termo *reutilização* e os seus parâmetros legais no que toca à publicação de imagem e som na *Internet* e nas redes sociais dos órgãos das autarquias locais.

Nos termos do Regulamento (UE) 2022/868, de 30 de maio[201], a «reutilização» [é] "a utilização, por pessoas singulares ou coletivas, de dados detidos por organismos do setor público, realizada para fins comerciais ou não comerciais que não correspondem à finalidade inicial da missão de serviço público para a qual os dados foram produzidos, excetuando o intercâmbio de dados entre organismos do setor público exclusivamente no desempenho das suas missões de serviço público;"

Este Regulamento, aplicável desde 24 de setembro de 2023, visa melhorar as condições de partilha de dados no mercado interno, criando um quadro harmonizado para o intercâmbio de dados e estabelecer determinados requisitos básicos para a governação de dados. O mesmo veio abranger novas situações de reutilização não abrangidas pela Diretiva 2019/1024, de 20 junho. Isto é, em termos gerais, a Diretiva 2019/1024 regula a reutilização de informações publicamente disponíveis na posse do setor público, enquanto, o Regulamento (EU) 2022/868 veio regulamentar a reutilização de outras grandes quantidades de dados protegidos (por exemplo, dados pessoais e dados comerciais confidenciais) onde é possível extrair uma grande riqueza de conhecimentos[202].

Ambos os documentos legislativos referem a importância de ter em conta o *RGPD* e os direitos dos titulares de dados pessoais. É de salientar que a regulamentação sobre a reutilização de dados abertos vem "[...] promover a transparência e a responsabilização dos organismos do setor público, bem como o crescimento económico, e não a transparência dos cidadãos."[203] Assim sendo, a reutilização, como operação de tratamento

---

[201] Relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados).

[202] Comissão Europeia, Explicação do Regulamento Governação de Dados.

[203] GT29 – Parecer 06/2013 sobre os dados abertos e a reutilização de informações do setor público («ISP»), p. 3.

de dados também tem de ter fundamento de licitude, que só poderá ser pela via do consentimento.

Para além disso, o Regulamento (EU) 2022/868 introduz o termo «altruísmo dos dados», que de acordo com o Art.º 2.º, ponto 16) consiste na "[...] partilha voluntária de dados, com base no consentimento dos titulares dos dados para o tratamento dos respetivos dados pessoais [...]".

No entanto, mesmo com o consentimento do titular, é necessário reter que a publicação de dados pessoais na *Internet* e nas redes sociais faz com que o responsável pelo tratamento, assim como o seu titular, percam o total controlo da informação disponibilizada.

Se mesmo a publicação de conteúdos com dados pessoais no sítio *web* institucional comporta o risco de reutilização indevida, este risco aumenta se forem publicados em plataformas que fogem ao controlo da Instituição. A par disso, a reutilização de imagens e voz poderá comportar a própria manipulação das mesmas por terceiros ao ponto de conseguirem modificar totalmente o que foi partilhado.

A perda de controlo, acima referida, acompanhada da acumulação de dados pessoais na *Internet* e a consequente facilidade de acesso, que se estende no tempo e no espaço, faz perigar os direitos do titular e coloca em causa os princípios inerentes à aplicabilidade do *RGPD*. Neste sentido, direitos como o direito ao apagamento, o direito de oposição e o direito à retificação são restringidos, em parte ou na totalidade, uma vez que o "paradeiro" dos dados dos titulares torna-se desconhecido. As plataformas digitais apropriam-se das informações publicadas que contemplam, na sua maioria, dados pessoais, colocando em causa princípios como o princípio da integridade e confidencialidade, o princípio da limitação das finalidades e o princípio da exatidão. Esta realidade intensifica, ainda mais, a falta de controlo por parte do responsável pelo tratamento quando divulga dados pessoais de terceiros em plataformas que não lhe pertencem.

Mais se acrescenta que esta falta de controlo acaba por interferir na verificação de responsabilidades. Questionamo-nos, a título meramente ilustrativo, quem é que poderá ser responsabilizado numa situação em que o titular retira o seu consentimento e se torna impossível efetivar o direito ao apagamento, consagrado no Art.º 17.º do *RGPD*?

Se, no contexto das redes sociais, é tarefa árdua (impossível até) saber para onde é que os dados pessoais são dirigidos, é de igual modo difícil perceber quantos responsáveis operam nos diferentes tipos de tratamento existentes nas plataformas em linha. Apesar das indicações explanadas no n.º 2 do Art.º 17.º do *RGPD*[204], é certo que a própria evolução da tecnologia e o crescente aumento de intervenientes nessas áreas dificulta todo o processo de eliminação de conteúdos. Por conseguinte, quando um titular retira o seu consentimento, torna-se impossível comunicar tal decisão aos diversos responsáveis pelo tratamento dos dados pessoais constantes nessas plataformas.

Em situações como esta, o direito ao apagamento é colocado em causa e a sua materialização é somente uma ilusão. Se assim o é, não restam dúvidas quanto a estarmos perante uma situação de incumprimento do *RGPD*. O direito do titular é violado pela sua impossibilidade de concretização e a consequente aplicação de sanções é ineficaz[205].

Além do mais, destacamos que este tipo de publicações em linha não poderão cumprir o princípio da limitação da conservação. Este princípio consagra que os dados pessoais devem ser conservados apenas durante o período necessário para as finalidades para as quais são tratados. Ora, como podemos observar, estando estes dados na *Internet* e nas redes sociais a sua conservação é permanente.

---

(204) *"Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do 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.".*

(205) COSTA, Tiago Branco da – O altruísmo (económico?) de dados: breves considerações sobre o espaço europeu de dados de saúde e a proteção de dados pessoais, p. 627.

Face ao exposto, o responsável pelo tratamento tem a obrigação de ponderar a necessidade de publicação, limitando ao máximo os conteúdos divulgados na *Internet* e nas redes sociais, nomeadamente quando está em causa a proteção de dados pessoais. Esta especificação e limitação da finalidade serve para travar o fenómeno "desvirtuamento da função", isto é, o alargamento ou a diluição progressiva das finalidades para as quais os dados são processados, após o titular de dados ter concordado com a recolha inicial dos dados. Apesar da existência de consentimento como um fundamento legítimo para o tratamento, a verdade é que existe sempre a possibilidade de ocorrer uma utilização imprevista dos dados pessoais pelo responsável pelo tratamento ou por terceiros, reforçando-se, nestes casos, a perda de controlo por parte do titular dos dados[206].

4. Necessidade de Avaliação de Impacto sobre Proteção de Dados

Tendo em conta esta realidade, não podemos deixar de referir a necessidade de se proceder a uma Avaliação de Impacto sobre a Proteção de Dados (AIPD), descrita no Art.º 35.º do *RGPD*. "Uma AIPD é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais, avaliando-os e determinando as medidas necessárias para fazer face a esses riscos. [...][207]. Para além de ajudar os responsáveis pelo tratamento a cumprir os requisitos do *RGPD*, são também instrumentos que demonstram que foram tomadas medidas adequadas para assegurar a conformidade com o mesmo[208].

---

[206] CEPD – Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679, parágrafo 56.

[207] GT 29 – Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, p. 4.

[208] GT 29 – Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, p. 4.

É obrigatório proceder a uma AIPD nos casos elencados no n.º 3 do Art.º 35.º do *RGPD*. Por seu turno, é de igual modo obrigatória nas situações listadas no Regulamento 798/2018 da CNPD, conforme o n.º 4 do Art.º 35.º do *RGPD*. Nesta lista, destacamos o exposto no número 2) – "[...] tratamento que relacione dados pessoais previstos no n.º 1 do Art.º 9.º [do *RGPD*] [...] ou dados de natureza altamente pessoal"[209].

O n.º 7 do Art.º 35.º do *RGPD* indica as informações mínimas que deverão constar de uma AIPD, sendo que a não conformidade pode conduzir à imposição de coimas pela autoridade de controlo competente. Para além disso, de acordo com o Art.º 36.º do *RGPD*, " o responsável pelo tratamento deve consultar a CNPD antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados [AIPD] [...] indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco".

IV. MEDIDAS NECESSÁRIAS

Tendo em conta as condições requeridas pelo *RGPD*, no que toca ao tratamento de dados no âmbito da captação de imagem e voz, o responsável pelo tratamento deve tomar as medidas técnicas e organizativas adequadas para a defesa dos direitos fundamentais dos titulares dos dados.

Por princípio, é aconselhada a não publicação de dados pessoais de cidadãos na *Internet*, principalmente nas redes sociais, pelas autarquias locais, visto não haver obrigação legal de cobertura mediática para as suas ações e iniciativas.

Ainda assim, a decisão de publicação de dados pessoais nas redes sociais, que implica a partilha de dados pessoais não imprescindíveis para a finalidade definida, necessita de ser ponderada através da elaboração

---

[209] Os "Dados de natureza altamente pessoal" são considerados sensíveis, associados a atividades privadas e familiares.

GT 29 – Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, p. 11.

de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD), que ajudará na determinação dos níveis de risco de segurança e privacidade.

Se após a análise dos resultados da AIPD, o responsável decidir efetuar a partilha de dados pessoais, não imprescindíveis para a finalidade, com terceiros (por exemplo, determinada publicação com vista à materialização do princípio da administração aberta) é necessário recolher o consentimento junto do titular dos dados, sendo este o único fundamento de licitude válido para este tipo de tratamento.

Aquando desta recolha é muito importante o cumprimento do dever de informação, nos termos do Art.º 13.º do *RGPD*, fornecendo as informações elencadas no seu n.º 1 e 2, através de uma linguagem clara e simples (Art.º 12.º, n.º 1 do *RGPD*). Esta obrigação de informar tem de ser cumprida antes da participação do cidadão no evento que poderá ser objeto de captação de imagem e/ou som e consequente publicação. Destaca-se aqui a importância de informar sobre a finalidade do tratamento de dados e da sua possível reutilização. Deve considerar-se, ainda, uma atenção redobrada quanto à recolha de dados pessoais de crianças, sendo obrigatório obter a devida autorização dos respetivos representantes legais.

O responsável pelo tratamento de dados tem de estar preparado para a possibilidade de os titulares não consentirem na gravação, transmissão ou divulgação da sua imagem e voz. Nestes casos, devem ser tomadas as medidas logísticas para respeitar este não consentimento. De referir que, quando não haja consentimento e se verifique inadvertidamente a captação de imagem e som do titular, o responsável deve proceder à sua eliminação, sendo proibida qualquer tipo de divulgação dos respetivos conteúdos.

Ainda quanto a estas matérias, é importante referir que, mesmo com o consentimento, o responsável pelo tratamento tem de ter em conta os princípios do *RGPD*, como o da minimização dos dados (Art.º 5.º, n.º 1, alínea c) do *RGPD*), não podendo recolher nem publicitar mais dados pessoais do que os necessários para a finalidade pretendida.

Para além disso, o responsável pelo tratamento deve assegurar a proteção dos dados desde a conceção e por defeito adotando as medidas técnicas e organizativas adequadas, incluindo as garantias necessárias para o tratamento, devendo ser capaz de o poder comprovar (n.º 2 do Art.º 5.º do *RGPD*). Só desta forma poderá cumprir o *RGPD* e proteger os direitos dos titulares dos dados pessoais.

Conclusão

A elaboração do presente artigo teve como objetivo central a análise e reflexão sobre a publicação de imagem (de fotografias e vídeos) e da voz (de áudios e/ou vídeos) nas redes sociais dos órgãos das autarquias locais, nomeadamente em plataformas como o *Facebook, Youtube* e *Instagram*. Neste sentido, procurámos analisar a relação existente entre os princípios da administração aberta e da proteção de dados pessoais.

Tivemos oportunidade de observar que a Administração Pública deve primar pela aplicabilidade de princípios estruturantes que permitam reforçar a transparência e a publicidade da sua atuação. Não obstante, não poderemos admitir que, em nome da administração aberta, se coloque em causa os direitos dos cidadãos. O escrutínio público pode ser considerado uma consequência natural e automaticamente aceite por quem se expõe publicamente no decorrer das suas funções laborais ou de forma "voluntária", mas isto não poderá ser sinónimo de abdicar sem reservas da proteção dos dados do cidadão em causa. Aceitar a total desproteção de dados pessoais de um determinado titular com o fundamento da transparência, da publicidade e da administração aberta poderá conduzir-nos a caminhos perigosos e irreversíveis.

Os órgãos autárquicos, como responsáveis pelo tratamento, têm a obrigação de proceder de acordo com o *RGPD* e de proteger ao máximo os dados pessoais (como a voz e a imagem) dos seus cidadãos, procedendo deste modo a um equilíbrio entre a transparência administrativa e o direito de acesso à informação através de meios eletrónicos, não descurando a proteção de dados pessoais. Não olvidamos que a exposição da vida privada de um titular poderá sofrer um maior impacto negativo se tal for publicada em redes sociais e na *Internet*, tendo em conta que há sempre a possibilidade de reutilização e difusão por terceiros dessas informações. Portanto, neste debate a preocupação com a proteção de dados pessoais deve ser acrescida.

Em suma, a proteção de dados pessoais é um direito do cidadão e um dever do responsável pelo tratamento, devendo este assegurar que o tratamento de dados pessoais é realizado de forma lícita, leal e transparente em relação

ao titular dos dados, limitado à finalidade da recolha e tratados de modo a garantir a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando-se as medidas técnicas ou organizativas adequadas à manutenção da sua integridade e confidencialidade.

Referências

Artigos

CARVALHO, Dina Sofia Martins; DANIEL, Ana Cristina Marques "As Redes Sociais e a Administração Pú-blica", *Revista Internacional de Gestão, Direito e Turismo* [Em linha]. N.º 12, junho. Escola Superior de Gestão de Idanha-a-Nova, 2016. ISSN 1645-2534. Disponível em <URL: https://gestin.ipcb.pt/wp-con-tent/uploads/2022/02/2016Gestin12art07.pdf>

DIAS, José Eduardo Figueiredo – Direito à informação, proteção da intimidade e autoridades administrativas independentes. In *Estudos em homenagem ao Prof. Doutor Rogério Soares* [Em linha]. Coimbra: Coimbra Editoria, 2001. ISBN: 9789723210507. Disponível em <URL: https://estudogeral.uc.pt/bi-tstream/10316/3497/1/protec%c3%a7%c3%a3o.pdf>

FARINHO, Domingos Soares – Interesse público e exercício da autoridade pública como fundamentos de li-citude de tratamento de dados pessoais. In FARINHO, Domingos Soares; MARQUES, Francisco Paes; FREI-TAS, Tiago Fidalgo – *Direito da Proteção de Dados: Perspetivas Públicas e Privadas*. Almedina, 2023. ISBN: 9789894012337.

COSTA, Tiago Branco da – O altruísmo (económico?) de dados: breves considerações sobre o espaço europeu de dados de saúde e a proteção de dados pessoais. 2022

Livros

BOTELHO, José Manuel Santos Botelho; ESTEVES, Américo Pires; PINHO, José Cândido de – *Código do Procedimento Administrativo anotado e comentado,* 4. ed. Coimbra: Almedina, 2000. ISBN 9724012921

CANOTILHO, Gomes; MOREIRA, Vital – *Constituição da República Portuguesa anotada.* 4. ed. Coimbra: Coimbra editora, 2014. ISBN 9789723222869.

CORDEIRO, António Barreto Menezes – *Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019*. Almedina, 2020. ISBN 9789724083049.

MAGALHÃES, Filipa Matias – O Princípio da Administração Aberta e o Direito à Proteção de Dados Pessoais: direitos conflituantes ou um direito duplamente garantístico. In *Estudos de e. governação, transparência e proteção de dados.* Coimbra: Almedina, 2021. ISBN: 9789724090269

MONIZ, Graça Canto – *Manual de Introdução à Proteção de Dados Pessoais*. Almedina, 2023. ISBN 9789894010487.

Websites

COMISSÃO EUROPEIA – *Commercial sector: adequacy decision on the EU-US Data Privacy Framework* [em linha]. 2023, atual. 2023. [Consult. 21 set. 2023]. Disponível em: <URL: https://commission.eu-ropa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en>.

COMISSÃO EUROPEIA – *Explicação do Regulamento Governação de Dados* [em linha]. 2023, atual. 2023 [Consult. 28 set. 2023]. Disponível em <URL: Explicação do Regulamento Governação de Dados | Shaping Europe's digital future (europa.eu)>

NYOB – *European Commission gives EU-US data transfers third round at CJEU* [Em linha]. 2023, atual. 2023.[Consult. 1 set. 2023]. Disponível em: <URL: https://noyb.eu/en/europe-an-commission-gives-eu-us-data-transfers-third-round-cjeu)

Legislação

CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA
JO 2016/C 202/02. (2000-12-07)

CÓDIGO DO PROCEDIMENTO ADMINISTRATIVO n.º 4/25
D.R. I Série. (2015-01-07)

CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA n.º 86/1976
D.R. I Série. (1976-04-10)

DELIBERAÇÃO n.º 427/AML/2022
Regimento da Assembleia Municipal de Lisboa. 35/CM/2008
deliberação. (2022-09-06)

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. *Regulamento geral sobre a proteção de dados.* (2016-04-27).

REGULAMENTO (UE) 2022/868 DO PARLAMENTO EUROPEU E DO CONSELHO de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724. *Regulamento Governação de Dados.* (2022-05-30).

REGULAMENTO (UE) 2022/2065 DO PARLAMENTO EUROPEU E DO CONSELHO de 19 de outubro de 2022 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE. *Regulamento dos Serviços Digitais.* (2022-10-19)

Websites

Parecer n.º 139/2021 - Processo n.º: 358/2021 de 19 de maio
Parecer n.º 253/2021 Processo n.º 352/2021 de 8 de setembro
Parecer n.º 44/2023, Processo n.º 785/2022 de 22 de fevereiro
Parecer n.º 73/2023 Processo n.º 976/2022 de 15 de março

Acórdãos

Tribunal de Justiça da União Europeia

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, **Schrems,** C-362/14, EU:C:2015:650 (2015-10-06)

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, ***Facebook,*** **Ireland** e **Schrems,** C-311/18, EU:C:2020:559 (2020-07-16).

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, FASHION ID, C-40/17, EU:C:2019:629 (2019-07-29)

Supremo Tribunal de Justiça

ACÓRDÃO DO SUPREMO TRIBUNAL DE JUSTIÇA n.º 0870/17. D.R. (2017-10-09).

Pareceres Diretrizes e Orientações

AUTORIDADE EUROPEIA DE PROTEÇÃO DE DADOS (AEPD), *Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679* [Em linha], WP259 rev.01, 17PT. 2020. Disponível em: <URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf>

COMISSÃO DE COORDENAÇÃO E DESENVOLVIMENTO REGIONAL DO CENTRO (CCDRC) – *Parecer Jurídico DSAJAL158/16*, 12 de agosto de 2016. Disponível em: <URL: https://www.ccdrc.pt/index.php?op-tion=com_pareceres&view=details&id=2211&Itemid=45>

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS (GT29), *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679* [Em linha], WP 248 rev.01, 17/PT. 2017.Disponível em: <URL: https://www.cnpd.pt/media/f0ide5i0/aipd_wp248rev-01_pt.pdf

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS (GT29), *Parecer 06/2013 sobre os dados abertos e a reutilização de informações do setor público («ISP»)* [em linha] WP207, 1021/00/PT. 2013. Disponível em <URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_pt.pdf>

Vídeos

ARTV – *Audição da Comissão Nacional de Proteção de Dados* (CNPD) [Em linha]. 30 de maio de 2023. Dis-ponível em <URL: https://canal.parlamento.pt/?cid=7083&-title=audicao-da-comissao-nacional-de-prote-cao-de-dados-cnpd>

ARTV – *Audição da Associação Nacional de Assembleias Municipais* (ANAM) [Em linha]. 30 de maio de 2023. Disponível em <URL: canal.parlamento.pt/?cid=7084&title=au-dicao-da-associacao-nacional-de-assembleias-municipais-anam>

7 | DA PUBLICAÇÃO NA INTERNET DAS ATAS DE REUNIÕES DE ÓRGÃOS COLEGIAIS AUTÁRQUICOS: UMA LEITURA (CRÍTICA) DA ORIENTAÇÃO DE 18 DE ABRIL DE 2023 DA CNPD

*Isabel Celeste M. Fonseca**
*Joel A. Alves***

Sumário

Resumo

Tendo como mote a Orientação de 18 de abril de 2023 da CNPD, relativa à publicação na *Internet* das atas de reuniões de órgãos colegiais, o presente artigo visa refletir sobre as restrições a que poderá ser sujeito o acesso a atas de órgãos colegiais administrativos – em especial, órgãos autárquicos – das quais constem dados pessoais. Para tanto, começar-se-á por apresentar o regime-geral traçado pela LADA, quanto ao acesso a documentos administrativos (§1). De seguida, procurar-se-á analisar como tal regime tem sido concretamente aplicado pela CADA, nos casos em que esteja em causa o acesso a atas de órgãos colegiais da Administração Pública (§2). Por fim, colocar-se-á a tónica na supramencionada orientação de 18 de abril de 2023 da CNPD, efetuando uma leitura crítica sobre o posicionamento jurídico nela sufragado (§3). Terminar-se-á com algumas notas conclusivas, procurando, essencialmente, dar resposta a duas interrogações fundamentais: poderá a publicação de atas de reuniões de órgãos colegiais locais na *Internet* considerar-se juridicamente admissível? Em caso afirmativo, sob que condições? (§4).

Palavras-chave

Atas; documentos administrativos; documentos nominativos; dados pessoais; transparência; informação reservada.

---

* Professora Associada da Escola de Direito da Universidade do Minho. Investigadora Principal no âmbito do projeto «Smart Cities and Law, E.Governance and Rights: Contributing to the definition and implementation of a Global Strategy for Smart Cities», ref. NORTE-01-0145-FEDER-000063.

** Assistente Convidado na Escola de Direito da Universidade do Minho. Doutorando em Ciências Jurídicas, na especialidade de Ciências Jurídicas Públicas, na Escola de Direito da Universidade do Minho. A colaboração no presente escrito foi efetuada com o apoio financeiro da Fundação para a Ciência e Tecnologia, ao abrigo da Bolsa de Investigação para Doutoramento melhor identificada pela referência 2022.13673.BD.

§0. Enquadramento

Na prossecução das atribuições que lhe são cometidas, enquanto autoridade de controlo nacional para efeitos do Regulamento Geral sobre a Proteção de Dados[210] e da Lei n.º 58/2019, de 8 de agosto[211], veio a Comissão Nacional de Proteção de Dados (=CNPD) recentemente aprovar cinco orientações dotadas de especial relevância para o setor público[212].

De entre estas, conta-se, designadamente, a Orientação de 18 de abril de 2023, relativa à publicação na *Internet* das atas de reuniões de órgãos colegiais. Matéria que, não sendo nova[213], continuara, nas palavras da referida entidade administrativa, a revelar-se "frequentemente objeto de consulta e de pedido de esclarecimentos"[214]. O que, na sua ótica, justificara levar a um público mais vasto o que viera sendo o seu entendimento sobre a mesma[215].

Tendo isso como mote, o presente artigo visa refletir sobre as restrições a que poderá ser sujeito o acesso a atas de órgãos colegiais administrativos – em especial, órgãos autárquicos – das quais constem dados pessoais. Para tanto, começar-se-á por apresentar o regime-geral traçado pela Lei de Acesso aos Documentos Administrativos[216], quanto ao acesso a documentos administrativos (§1). De seguida, procurar-se-á analisar como tal regime tem sido concretamente aplicado pela Comissão de Acesso aos

---

(210) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que respeita ao tratamento de dados pessoais e à livre circulação desses dados (de ora em diante, abreviadamente designado por *RGPD*).

(211) Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do *RGPD*.

(212) Cfr. CNPD, "Novas orientações da CNPD", 5 de maio de 2023, disponível em https://www.cnpd.pt/comunicacao-publica/noticias/novas-orientacoes-da-cnpd/ [Consultado a 11 de maio de 2023].

(213) Sobre o tema, vd. Acórdão da Relação do Porto de 07/11/2019 RP2019111071606/17.4T8PVZ.P1, disponível em www.dgsi.pt, consultado em 23 de janeiro de 2020 (IV – A quebra do segredo profissional e o acesso da ATA a dados sobre factos da vida íntima dos cidadãos não depende de permissão da Lei da Protecção de Dados Pessoais. V – A Lei da Protecção de Dados Pessoais não impede a comunicação dos dados a terceiros desde que nessa comunicação exista um objectivo legítimo que seja susceptível de justificar uma ingerência na vida privada, o que cabe às ordens jurídicas nacionais definir).

(214) Idem.

(215) Idem.

(216) Lei n.º 26/2016, de 22 de agosto, que prova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos, transpondo a Diretiva 2003/4/CE, do Parlamento Europeu e do Conselho, de 28 de janeiro, e a Diretiva 2003/98/CE, do Parlamento Europeu e do Conselho, de 17 de novembro (de ora em diante, abreviadamente designada por LADA).

Documentos Administrativos (=CADA), nos casos em que esteja em causa o acesso a atas de órgãos colegiais da Administração Pública (§2). Por fim, colocar-se-á a tónica na supramencionada orientação de 18 de abril de 2023 da CNPD, efetuando uma leitura crítica sobre o posicionamento jurídico nela sufragado (§3). Terminar-se-á com algumas notas conclusivas, procurando, essencialmente, dar resposta a duas interrogações fundamentais: poderá a publicação de atas de reuniões de órgãos colegiais locais na *Internet* considerar-se juridicamente admissível? Em caso afirmativo, sob que condições? (§4).

§1. O regime-geral da LADA

1.1. A regra do livre acesso

Dito isto, importa recordar que as atas das reuniões de órgãos autárquicos configuram documentos administrativos, na aceção do artigo 3.º, n.º 1, alínea a), da LADA[217]. Donde, salvo legislação específica em contrário, a sua disponibilização deva necessariamente realizar-se de acordo com as condições gerais de acesso, consagradas nesse mesmo diploma[218].

Nesta senda, estabelece o artigo 5.º, n.º 1, da LADA, enquanto regime-regra, que "todos, sem necessidade de enunciar qualquer interesse, têm direito de acesso aos documentos administrativos". O que significa que, por princípio, qualquer documento "diretamente produzido ou recolhido no exercício normal de funções administrativas"[219] – i.e. que haja sido elaborado ou se encontre na posse "de entidades públicas ou

---

[217] Nesse sentido, cfr., entre outros, CADA, Parecer n.º 214/2023, Processo n.º 5/2023, 19 de julho de 2023, p. 2; CADA, Parecer n.º 111/2023, Processo n.º 10009/2022, 19 de abril de 2023, p. 2; CADA, Parecer n.º 365/2021, Processo n.º 445/2021, 16 de dezembro de 2021, p. 1.

[218] Para mais desenvolvimentos, cfr. PRATAS, Sérgio, *A (nova) Lei de Acesso aos Documentos Administrativos*, Almedina, Coimbra, 2018, p. 66.

[219] Seguimos aqui a noção de "documento administrativo" proposta por CAUPERS, João, "Sobre o conceito de documento administrativo", in *Cadernos de Justiça Administrativa,* n.º 75, p. 9. Definição essa que, aliás, tem sido reiteradamente acolhida pela jurisprudência dos tribunais administrativos superiores portugueses. Nesse sentido, veja-se, entre outros arestos, (i) o Acórdão do STA (1.ª Secção de Contencioso Administrativo), de 10 de março de 2022, Processo n.º 02063/21.6BELSB; (ii) o Acórdão do STA (1.ª Secção de Contencioso Administrativo), de 10 de setembro de 2014, Processo n.º 0410/14; e (iii) o Acórdão do TCA-N (1.ª Secção de Contencioso Administrativo), de 20 de dezembro de 2019, Processo n.º 01414/19.8BEPRT.

privadas, por efeito da sua atuação, ainda que circunstancial, no exercício de prerrogativas de autoridade ou segundo um regime de direito administrativo"[220] – deve presumir-se "de acesso livre e irrestrito"[221].

A justificação para tal é simples. Afinal, conquanto não goze de positivação expressa na Constituição da República Portuguesa ou no Código do Procedimento Administrativo[222], é hoje pacífico que o *princípio da transparência da atividade administrativa* se apresenta como um elemento "consubstancial a toda a ordem jurídica democrática"[223], "constituindo mesmo condição indispensável para o exercício da cidadania e da participação na vida pública e para a responsabilização *(accountability)* e o controlo externo dos poderes públicos"[224].

Dito de outro modo: não sofre hoje controvérsia que "só num sistema administrativo inspirado pela transparência se pode realizar, na sociedade, uma efetiva atividade propositiva, participativa e de controlo, bem como o valor da cidadania administrativa"[225]. Daí a comum asserção de que uma Administração democrática não pode deixar de afirmar-se como uma *Administração transparente*[226]; uma verdadeira "casa de vidro"[227], que, muito embora não prescindindo de "algumas janelas protegidas

---

[220] Cfr. ALMEIDA, Mário Aroso de / CADILHA, Carlos Alberto Fernandes, *Comentário ao Código de Processo nos Tribunais Administrativos,* 4.ª edição, Almedina, Coimbra, 2017, p. 857.

[221] Sublinhando que é este o princípio-geral aplicável em matéria de acesso a documentos administrativos, por força do disposto no artigo 5.º, n.º 1, da LADA, cfr. CADA, Parecer n.º 357/2021, Processo n.º 752/2021, 16 de dezembro de 2021, p. 5.

[222] Alertando para tal facto, cfr. FARINHO, Domingos Soares, "Princípio da administração aberta: a evolução do direito positivo português", in *O Acesso à Informação Administrativa* (org. Tiago Fidalgo de Freitas / Pedro Delgado Alves), Almedina, Coimbra, 2021, p. 12; FERNANDES, Débora Melo, "O princípio da transparência administrativa: mito ou realidade?", *Revista da Ordem dos Advogados,* Ano 75, Jan-Jul 2015, pp. 427-429.

[223] Nesse sentido, cfr. Acórdão do Tribunal Constitucional (1.ª secção), de 30 de junho de 1992, Processo n.º 34/90.

[224] Cfr. FERNANDES, Débora Melo, "O princípio da transparência administrativa: mito ou realidade?", *Revista da Ordem dos Advogados,* Ano 75, Jan-Jul 2015, p. 427.

[225] Cfr. GONÇALVES, Pedro Costa, Manual de Direito Administrativo, vol. 1, Almedina, Coimbra, 2019, p.485.

[226] Nesse sentido, cfr. MORÓN, Miguel Sánchez, *Derecho Administrativo: parte general,* 16.ª edição, Tecnos, Madrid, p. 81.

[227] Cfr. ANTUNES, Luís Filipe Colaço, "Mito e realidade da transparência administrativa", in Boletim da Faculdade de Direito da Universidade de Coimbra, 1993, p. 16.

ou fechadas"[228], promove uma cultura de tendencial abertura e revelação, permitindo aos cidadãos saberem o que ela sabe[229], para, assim, averiguarem da *legalidade* e *mérito* da sua atuação[230].

Daqui decorre que, quaisquer órgãos e entidades cobertos pelo âmbito de aplicação subjetivo da LADA – como sejam, para o que aqui importa, os órgãos das autarquias locais[231] – "têm, quando solicitados, o dever de facultar a sua documentação administrativa"[232].

Mais: independentemente dos pedidos que lhes sejam dirigidos, impõe-se a tais órgãos e entidades que coloquem em prática "uma política ativa de informação aberta e transparente que facilite e promova o controlo difuso da sua ação pelos cidadãos"[233] – assim o determina o artigo 2.º, n.º 2, da LADA, onde se lê que "a informação pública relevante para garantir a transparência da atividade administrativa, designadamente a relacionada com o funcionamento e controlo da atividade pública" deve ser "divulgada ativamente, de forma periódica e atualizada, pelos respetivos órgãos e entidades". Obrigação que o artigo 10.º, n.º 1, do mesmo diploma complementa e concretiza, estabelecendo que, para o efeito, tais órgãos e entidades devem, nomeadamente, publicitar nos seus sítios na *Internet*, de forma periódica e atualizada, no mínimo semestralmente, "os documentos administrativos (...) que entendam disponibilizar livremente para acesso e reutilização", bem como toda "a informação cujo conhecimento seja relevante para garantir a transparência da atividade relacionada com o seu funcionamento".

---

[228] Idem, ibidem.

[229] Cfr. AMORIM, João Pacheco / OLIVEIRA, Mário Esteves de / GONÇALVES, Pedro Costa, *Código do Procedimento Administrativo – Comentado,* Almedina, Coimbra, 2010, p. 342.

[230] Em sentido próximo, sustentando que "a promoção da transparência funciona como fator de controlo da própria vinculação da Administração à legalidade e ao mérito", cfr. FARINHO, Domingos Soares, "Princípio da administração aberta: a evolução do direito positivo português", in *O Acesso à Informação Administrativa* (org. Tiago Fidalgo de Freitas / Pedro Delgado Alves), Almedina, Coimbra, 2021, p. 18.

[231] Cfr. artigo 4.º, n.º 1, alínea e), da LADA.

[232] Cfr. Acórdão do STA (1.ª Secção do Contencioso Administrativo), de 6 de janeiro de 2010, Processo n.º 0965/09.

[233] CCfr. GONÇALVES, Pedro Costa, Manual de Direito Administrativo, vol. 1, Almedina, Coimbra, 2019, p.485.

1.2. As restrições aplicáveis ao acesso a documentos administrativos nominativos

Se é certo que na atividade administrativa a regra deve ser a informação e não o segredo[234], tal não significa, porém, que os órgãos e entidades anteriormente referidos não possam, face a certas circunstâncias, limitar o acesso à documentação administrativa na sua posse. É que, sendo embora um *direito fundamental de natureza análoga aos direitos, liberdades e garantias*[235], "o direito de acesso aos documentos administrativos não é um direito absoluto, pois pode colidir com outros bens ou direitos legalmente protegidos"[236]. Circunstância que pode, naturalmente, justificar a sua restrição, por forma a que seja assegurada a necessária concordância prática entre todos os valores jurídicos em confronto.

Ora, é precisamente o que se verifica quanto aos designados "documentos nominativos", isto é, documentos administrativos que contenham dados pessoais, na aceção do artigo 4.º, n.º 1, do *RGPD*[237]. Documentos esses que, no respeito pelo disposto no artigo 35.º da Constituição da República

---

[234] Nesse sentido, veja-se, entre outros, o Acórdão do STA de 20 de janeiro de 2010, Processo n.º 01110/09, bem como o Acórdão do STA (1.ª Subsecção do Contencioso Administrativo) de 30 de setembro de 2009, Processo n.º 0493/09, e o Acórdão do STA (1.ª Subsecção do Contencioso Administrativo) de 17 de janeiro de 2008, Processo n.º 0896/07.

[235] Cfr., *inter alia,* o Acórdão do STA (2.ª Subsecção do Contencioso Administrativo), de 21 de setembro de 2010, Processo n.º 0562/10, bem como o Acórdão do TCA-N (1.ª Secção do Contencioso Administrativo), de 13 de julho de 2012, e o Acórdão do TCA-S (1.ª Secção do Contencioso Administrativo), de 19 de outubro de 2017, Processo n.º 856/17.8BELRA.

[236] Cfr. Acórdão do TCA-S (1.ª Secção do Contencioso Administrativo), de 4 de novembro de 2010, Processo 06744/10. Em sentido idêntico, veja-se, ainda o Acórdão do STA (2.ª Subsecção do Contencioso Administrativo), de 8 de julho de 2009, Processo n.º 0451/09, bem como o Acórdão do TCA-N (1.ª Secção do Contencioso Administrativo), de 14 de fevereiro de 2007, Processo n.º 01180/06.7BEPRT.

[237] Cfr. artigo 3.º, n.º 1, alínea b), da LADA. Recorde-se que, nos termos do supramencionado artigo 4.º, n.º 1 do *RGPD*, entende-se por dados pessoais qualquer "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)". Sendo que, de acordo com o mesmo preceito, deve considerar-se "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". Para mais desenvolvimentos, cfr., com as necessárias adaptações, Grupo de Trabalho de Proteção de Dados do Artigo 29.º, "Parecer 4/2007 sobre o conceito de dados pessoais", 20 de junho de 2007.

Portuguesa – e, em especial, pelo princípio vertido no seu n.º 4, segundo o qual "é proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei" –, o legislador entendeu submeter a um regime específico de proteção.

Assim, e em derrogação da regra-geral de livre acesso, prevista no seu artigo 5.º, n.º 1, dispõe o artigo 6.º, n.º 5, da LADA, que um terceiro só tem direito de acesso a documentos administrativos nominativos: (i) 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; ou (ii) se demonstrar fundamentadamente ser titular de um interesse, direto, pessoal, legítimo e constitucionalmente protegido suficientemente relevante que, após ponderação, no quadro do princípio da proporcionalidade, de todos os direitos fundamentais em presença e do princípio da administração aberta, justifique o acesso à informação.

Sem embargo, deixa o artigo 6.º, n.º 9, do mesmo diploma, ainda assim, ressalvado 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". O que aponta para a aplicação de um regime jurídico diferenciado, consoante esteja em causa o acesso a documentos administrativos que contenham *dados pessoais de categorias especialmente protegidas* – seja nos termos do *RGPD*[238], seja nos termos do nosso texto constitucional[239] – ou o «mero» acesso a documentos administrativos que contenham *dados pessoais de categorias comuns*[240].

---

[238] CCfr. artigo 9.º, n.º 1, do *RGPD*.

[239] Cfr. artigo 35.º, n.º 3, da Constituição da República Portuguesa.

[240] Em sentido idêntico, cfr. FABIÃO, Gonçalo de Andrade, "Restrições de acesso à informação administrativa: dados pessoais", in *O Acesso à Informação Administrativa* (coord. Tiago Fidalgo de Freitas / Pedro Delgado Alves), Almedina, Coimbra, 2021, pp. 225-226.

Passamos a explicar. Estando em causa documentos administrativos que contenham dados pessoais de categorias especialmente protegidas, será de aplicar integralmente o disposto no supramencionado artigo 6.º, n.º 5, da LADA. Pelo que, salvo a existência de autorização escrita do titular dos dados, prestada de acordo com as condições previstas nesse mesmo preceito, o acesso à documentação administrativa somente poderá ser concedido se o requerente demonstrar fundamentadamente ser titular de um interesse, direto, pessoal, legítimo e constitucionalmente protegido suficientemente relevante que, após ponderação, no quadro do princípio da proporcionalidade, de todos os direitos fundamentais em presença e do princípio da administração aberta, justifique o acesso à informação.

Já estando em causa documentos administrativos que «apenas» contenham *dados pessoais de categorias comuns,* o artigo 6.º, n.º 5, da LADA, deve ser lido em conjugação com o artigo 6.º, n.º 9, do mesmo diploma. O que quer dizer que, para aceder à documentação pretendida, "não é exigido que o requerente apresente interesse direto, pessoal, legítimo e constitucionalmente protegido diferente do direito de acesso a documentos administrativos"[241]. Antes lhe basta fazer uso deste direito e, bem assim, demonstrar, após ponderação, no quadro do princípio da proporcionalidade, que o seu exercício justifica, *in casu*, o sacrifício do direito à proteção de dados pessoais dos demais envolvidos[242].

§1. O regime-geral da LADA

Perante isto, tem a CADA entendido que "de uma forma geral, as atas de órgãos da Administração Pública são subsumíveis à regra de livre acesso, prevista no já citado artigo 5.º, n.º 1, da LADA"[243]. Contudo, nem por isso esta entidade administrativa deixa de reconhecer que pode existir nesses documentos "informação reservada, designadamente, de natureza nominativa e irrelevante à atividade administrativa, por isso, não livremente acessível"[244].

---

[241] Idem, p. 226.

[242] Idem, ibidem.

[243] Cfr. CADA, Parecer n.º 246/2023, Processo n.º 153/2023, 19 de julho de 2023, p. 4.

[244] Cfr. CADA, Parecer n.º 214/2023, Processo n.º 5/2023, 19 de julho de 2023, p. 3.

Exemplo disso é o que sucede com os números de identificação civil e fiscal, a morada, ou os números de telefone e telemóvel de pessoas singulares[245]. Tudo isto, *dados pessoais,* na aceção do artigo 4.º, n.º 1, do *RGPD*. E, bem assim, "elementos cujo conhecimento, em princípio, nada acrescentaria à faculdade de controlo da atividade administrativa"[246]. O que justifica que a sua disponibilização a terceiros possa ser objeto de restrições – contrariamente a outros *dados, de natureza meramente funcional,* tais como o nome dos membros dos órgãos públicos que participaram na reunião, os quais devem ser de acesso livre, em nome dos princípios da transparência e do controlo público da atividade administrativa[247].

Não obstante, ponto é que mesmo o acesso a atas onde constem *dados pessoais de natureza não meramente funcional* não deve ser condicionado na sua totalidade. De todo. Segundo a melhor jurisprudência da CADA, a obtenção da necessária concordância prática entre o *direito de acesso aos documentos administrativos* e o *direito à proteção de dados pessoais,* numa situação jurídico-factual com esse tipo de contornos, passa por uma solução diversa – qual seja, a disponibilização da documentação em causa com o expurgo da eventual informação de carácter reservado que nela possa existir[248]. Posicionamento que, diga-se, vai em linha com o previsto no artigo 6.º, n.º 8, da LADA, onde se lê que "os documentos administrativos sujeitos a restrições de acesso são objeto de comunicação parcial sempre que seja possível expurgar a informação relativa à matéria reservada".

De resto, estranho seria se assim não fosse. Afinal, para além de documentos administrativos, as atas de órgãos colegiais da Administração Pública constituem instrumentos aos quais o nosso ordenamento jurídico atribui uma específica *função de publicidade:* "as atas das reuniões de órgãos colegiais visam, por natureza, registar e dar a conhecer

[245] Idem, ibidem.

[246] Idem, pp. 4-5.

[247] Cfr. CADA, Parecer n.º 77/2021, Processo n.º 30/2021, 24 de março de 2021, p. 4.

[248] Nesse sentido, cfr., entre outros, CADA, Parecer n.º 73/2023, Processo n.º 976/2022, 15 de março de 2023, p. 3.

a emissão das deliberações tomadas nas reuniões dos órgãos colegiais"[249]. Assim resulta, de forma cristalina, do disposto no artigo 34.º, n.º 1, do Código do Procedimento Administrativo, nos termos do qual se estabelece que "de cada reunião é lavrada ata, que contém um resumo de *tudo o que nela tenha ocorrido e seja relevante para o conhecimento e a apreciação da legalidade das deliberações tomadas*" (destaque nosso).

Por outras palavras: as atas das reuniões de órgãos colegiais administrativos – tais como os órgãos das autarquias locais – existem, nada mais nada menos, do que para *levar ao conhecimento do público* tudo o que de relevante naquelas tenha ocorrido, designadamente, por forma a possibilitar o *controlo da legalidade* – e, quando tal se justifique, do próprio *mérito* – das deliberações ali tomadas. Objetivo que, evidentemente, estaria condenado ao fracasso, caso estas se configurassem como *documentos de acesso restrito*.

Nestes termos, o entendimento perfilhado pela CADA parece-nos não apenas lógico como equilibrado: "as atas são, em regra documentos de acesso livre. Se eventualmente nelas existir alguma matéria reservada, deve a mesma ser expurgada nessa parte"[250] – reitera-se, *apenas e só nessa parte,* sob pena de a restrição em causa se afigurar ilegítima, traduzindo-se numa injustificada denegação do direito de acesso aos documentos administrativos.

§3. A Orientação da CNPD de 18 de abril de 2023

Ocorre que, tal como a CNPD teve ocasião de advertir, no quadro da já citada orientação de 18 de abril de 2023, relativa à publicação na *Internet* das atas de reuniões de órgãos colegiais, a consulta das atas não se confunde com a respetiva publicação na *Internet*[251]. Isto porque, nas palavras da autoridade de controlo nacional, para efeitos do *RGPD* e da

---

[249] Cfr. CNPD, "Orientação relativa à publicação na Internet das atas das reuniões de órgãos colegiais", p. 1.

[250] Cfr. CADA, Parecer n.º 73/2023, Processo n.º 976/2022, 15 de março de 2023, p. 3.

[251] CNPD, "Orientação relativa à publicação na Internet das atas das reuniões de órgãos colegiais", p. 1.

Lei n.º 58/2019, de 8 de agosto, a divulgação de documentos administrativos que contenham dados pessoais na *Internet* "significa a permanente disponibilização de tais dados, muito para além do espaço territorial nacional e do período de tempo necessário, ou seja, do perímetro dos interessados e do período temporal pertinentes. A que acresce a circunstância de, nesse contexto de rede aberta, os dados pessoais serem ou poderem ser objeto de reutilização por qualquer um para qualquer finalidade, inclusive ilegítima, em face da dificuldade ou mesmo impossibilidade de rastrear o seu tratamento por terceiros. Demais, o relacionamento automático com outros dados relativos à mesma pessoa, permite ou potencia a criação de perfis sobre as pessoas e de subsequente tomada de decisões (ou de outros atos) que afetem diretamente a esfera jurídica dos seus titulares"[252].

Quer isto dizer, em suma, que a divulgação ativa de documentos administrativos nominativos na *Internet* comporta riscos substancialmente elevados[253], de todo incomparáveis com os que se verificam no panorama clássico em que a administração detém a informação, o particular pede o acesso e a informação é disponibilizada.

Circunstância que, naturalmente, determina a sua sujeição a um regime mais restritivo – sob pena de uma excessiva e intolerável compressão de direitos fundamentais como o direito à proteção de dados pessoais, o direito ao respeito pela vida privada, ou o direito à igualdade (na vertente de não discriminação) dos titulares das informações objeto de disseminação[254].

Nesta senda, a posição da CNPD é clara: por norma, a publicação de atas de órgãos colegiais administrativos na *Internet* apenas se deverá considerar admissível quando estas não contenham dados pessoais[255]. Estando em causa documentos nominativos, deve a documentação

[252] Idem, pp. 1-2.
[253] Idem, ibidem.
[254] Idem, p. 2.
[255] Idem, p. 3.

em jogo ser anonimizada – isto é, expurgada de todos os dados pessoais nela constantes – previamente à sua divulgação[256]. Caso contrário "a publicação na Internet não será admissível (...) atenta a repercussão que (...) pode ter na vida das pessoas visadas e considerando que existem meios capazes de garantir ainda o princípio da transparência, sem expor de modo permanente e para além do universo de potenciais interessados nas informações"[257].

O único desvio que a CNPD admite a este princípio-regra prende-se com a divulgação de atas que contenham deliberações administrativas que se encontrem legalmente sujeitas a publicação na *Internet* – tal como sucede, para o que aqui releva, com as *deliberações dos órgãos colegiais locais destinadas a ter eficácia externa*[258]. Nestes casos – sublinhe-se, apenas e só nestes casos – a autoridade de controlo nacional prefigura a publicação de atas com dados pessoais na *Internet* como possível, desde que realizada "em cumprimento dos princípios da proporcionalidade e da minimização dos dados, consubstanciados na alínea c) do n.º 1 do artigo 5.º do *RGPD*"[259]. O que, nas suas palavras, nomeadamente, implica que as atas a publicar sejam elaboradas "com a redução ao indispensável dos dados que integrem as categorias previstas no n.º 1 do artigo 9.º e no artigo 10.º do *RGPD* – por exemplo, eventuais decisões relativas a procedimentos disciplinares devem ser registadas em ata por referência ao número do processo, sem identificação do trabalhador visado"[260].

---

[256] Idem, ibidem.

[257] Idem, p. 2.

[258] Assim decorre do artigo 56.º da Lei n.º 75/2013, de 12 de setembro, onde se prescreve que "[p]ara além da publicação em Diário da República quando a lei expressamente o determine, as deliberações dos órgãos das autarquias locais, bem como as decisões dos respetivos titulares destinadas a ter eficácia externa, devem ser publicadas em edital afixado nos lugares de estilo durante cinco dos 10 dias subsequentes à tomada da deliberação ou decisão, sem prejuízo do disposto em legislação especial" (n.º 1). E, bem assim, que "[o]s atos referidos no número anterior são ainda publicados no sítio da Internet, no boletim da autarquia local e nos jornais regionais editados ou distribuídos na área da respetiva autarquia, nos 30 dias subsequentes à sua prática" (n.º 2).

[259] CNPD, "Orientação relativa à publicação na Internet das atas das reuniões de órgãos colegiais", p. 3.

[260] Idem, ibidem.

§4. Conclusões

Do exposto, podem, pois, extrair-se as seguintes conclusões:

i. Estando em causa o *acesso a atas de órgãos colegiais administrativos, através de pedido formulado nos termos do artigo 12.º, n.º 1, da LADA*, deve este ser concedido:

a. sempre que a documentação concretamente solicitada *não contenha dados pessoais*, e não se verifiquem outras restrições, previstas na LADA ou em legislação especial, que impeçam a sua disponibilização a terceiros;

b. sempre que a documentação concretamente solicitada *apenas contenha dados pessoais de natureza funcional* (*e.g.* identificação de quem esteve presente na reunião a que a ata se refere, e em nome de quem esteve presente);

c. sempre que a documentação concretamente solicitada c*ontenha outro tipo de dados pessoais*, na medida em que a entidade requerida proceda ao expurgo da informação de carácter reservado que nelas existas (*e.g.* números de identificação civil e fiscal; moradas; números de telefone e telemóvel de pessoas singulares; etc.), previamente à sua disponibilização.

ii. Existindo nas atas de órgãos colegiais administrativos *deliberações legalmente sujeitas a publicação na Internet* – tal como sucede com as deliberações dos órgãos colegiais locais destinadas a ter eficácia externa – devem as deliberações em questão ser ativamente divulgadas no *website* institucional de tais entidades. O que, todavia – e contrariamente ao que a CNPD parece sugerir, na sua orientação de 18 de abril de 2023, relativa à publicação na *Internet* das atas de reuniões de órgãos colegiais –, não implica que as atas nas quais essas deliberações se integram tenham, elas próprias, de ser publicadas. Pelo contrário: o que se exige é a divulgação ativa das deliberações. Não das atas, na sua globalidade.

iii. Na ausência de disposição legal específica, através da qual expressamente se comine a obrigatoriedade de *publicação na Internet das atas de órgãos colegiais administrativos,* apenas se poderá considerar tal publicação como admissível caso:

a. a documentação ativamente divulgada não contenha dados pessoais, ou qualquer outra informação sujeita a restrições de acesso, nos termos da LADA (*e.g.* segredos comerciais, industriais ou sobre a vida de uma empresa) ou de legislação especial (*e.g.* informação coberta pelo regime do segredo de Estado, aprovado pela Lei Orgânica n.º 2/2014, de 6 de agosto).

b. *contendo dados pessoais* – e/ou qualquer outra informação de carácter reservado – esses elementos sejam objeto de expurgo, previamente à publicação.

De facto, no que especificamente respeita a este último ponto, o artigo 10.º, n.º 5, da LADA é claro: "a divulgação ativa da informação deve acautelar o respeito pelas restrições de acesso previstas na presente lei, devendo ter lugar a divulgação parcial sempre que seja possível expurgar a informação relativa à matéria reservada". Solução que, diga-se, encontra-se em harmonia, quer com a 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 – onde se estabelece que os Estados-Membros devem incentivar os organismos do setor público e as empresas públicas a produzir e disponibilizar documentação em conformidade com o princípio «abertos desde a conceção e por defeito»[(261)] –, quer com o Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022, relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados) – onde, por sua vez, se determina que os organismos do setor público devem assegurar, em conformidade com o direito da União e nacional, que a natureza protegida dos dados que pretendam disponibilizar seja preservada; o que

[(261)] Cfr. artigo 5.º, n.º 2, da Diretiva.

pode justificar a adoção de requisitos, tais como os de que o acesso para fins de reutilização de dados apenas deverá ser concedido se o organismo do setor público ou o organismo competente, na sequência de um pedido de reutilização, *tiver assegurado que os dados foram anonimizados, no caso dos dados pessoais, ou foram alterados, agregados ou tratados por qualquer outro método de controlo da divulgação, no caso das informações comerciais confidenciais, incluindo os segredos comerciais ou conteúdos protegidos por direitos de propriedade intelectual*[262].

[262] Cfr. artigo 5.º, n.º 3, alínea a), do Regulamento.

Bibliografia

ALMEIDA, Mário Aroso de / CADILHA, Carlos Alberto Fernandes,
Comentário ao Código de Processo nos Tribunais Administrativos, 4.ª edição, Almedina, Coimbra, 2017.

AMORIM, João Pacheco / OLIVEIRA, Mário Esteves de / GONÇALVES, Pedro Costa,
Código do Procedimento Administrativo – Comentado, Almedina, Coimbra, 2010.

ANTUNES, Luís Filipe Colaço,
"Mito e realidade da transparência administrativa", in *Boletim da Faculdade de Direito da Universidade de Coimbra,* 1993, pp. 1-55.

CAUPERS, João,
"Sobre o conceito de documento administrativo", in *Cadernos de Justiça Administrativa,* n.º 75, pp. 3-10.

FABIÃO, Gonçalo de Andrade,
"Restrições de acesso à informação administrativa: dados pessoais", in *O Acesso à Informação Administrativa* (coord. Tiago Fidalgo de Freitas / Pedro Delgado Alves), Almedina, Coimbra, 2021, pp. 209-235.

FARINHO, Domingos Soares,
"Princípio da administração aberta: a evolução do direito positivo português", in *O Acesso à Informação Administrativa* (org. Tiago Fidalgo de Freitas / Pedro Delgado Alves), Almedina, Coimbra, 2021, pp. 7-29.

FERNANDES, Débora Melo,
"O princípio da transparência administrativa: mito ou realidade?", *Revista da Ordem dos Advogados,* Ano 75, Jan-Jul 2015, pp. 425-457.

GONÇALVES, Pedro Costa,
Manual de Direito Administrativo, vol. 1, Almedina, Coimbra, 2019, p.485.

MORÓN, Miguel Sánchez,
Derecho Administrativo: parte general, 16.ª edição, Tecnos, Madrid,

PRATAS, Sérgio,
A (nova) Lei de Acesso aos *Documentos Administrativos,* Almedina, Coimbra, 2018.

Jurisprudência citada

ASTA (1.ª Secção de Contencioso Administrativo),
Acórdão de 10 de março de 2022, Processo n.º 02063/21.6BELSB.
STA (1.ª Secção de Contencioso Administrativo),
Acórdão de 10 de setembro de 2014, Processo n.º 0410/14.
STA (2.ª Subsecção do Contencioso Administrativo),
Acórdão de 21 de setembro de 2010, Processo n.º 0562/10.
STA (1.ª Subsecção do Contencioso Administrativo),
Acórdão de 20 de janeiro de 2010, Processo n.º 01110/09.

STA (1.ª Secção do Contencioso Administrativo),
Acórdão de 6 de janeiro de 2010, Processo n.º 0965/09.
STA (1.ª Subsecção do Contencioso Administrativo),
Acórdão de 30 de setembro de 2009, Processo n.º 0493/09.
STA (2.ª Subsecção do Contencioso Administrativo),
Acórdão de 8 de julho de 2009, Processo n.º 0451/09.
STA (1.ª Subsecção do Contencioso Administrativo),
Acórdão de 17 de janeiro de 2008, Processo n.º 0896/07.
TCA-N (1.ª Secção de Contencioso Administrativo),
Acórdão de 20 de dezembro de 2019, Processo n.º 01414/19.8BEPRT.
TCA-N (1.ª Secção do Contencioso Administrativo),
Acórdão de 13 de julho de 2012.
TCA-N (1.ª Secção do Contencioso Administrativo),
Acórdão de 14 de fevereiro de 2007, Processo n.º 01180/06.7BEPRT.
TCA-S (Secção de Contencioso Administrativo),
Acórdão de 8 de setembro de 2022, Processo n.º 399/22.8BESNT.
TCA-S (Secção de Contencioso Administrativo),
Acórdão de 19 de outubro de 2017, Processo n.º 856/17.8BELRA.
TCA-S (1.ª Secção do Contencioso Administrativo),
Acórdão de 4 de novembro de 2010, Processo 06744/10.
Tribunal Constitucional (1.ª secção),
Acórdão de 30 de junho de 1992, Processo n.º 34/90.

Outros documentos

CADA, Parecer n.º 345/2023, Processo n.º 205/2023, 13 de setembro de 2023.
CADA, Parecer n.º 246/2023, Processo n.º 153/2023, 19 de julho de 2023.
CADA, Parecer n.º 214/2023, Processo n.º 5/2023, 19 de julho de 2023.
CADA, Parecer n.º 111/2023, Processo n.º 1009/2022, 19 de abril de 2023.
CADA, Parecer n.º 73/2023, Processo n.º 976/2022, 15 de março de 2023.
CADA, Parecer n.º 333/2022, Processo n.º 588/2022, 14 de setembro de 2022.
CADA, Parecer n.º 74/2022, Processo n.º 692/2021, 16 de março de 2022.
CADA, Parecer n.º 365/2021, Processo n.º 445/2021, 16 de dezembro de 2021.
CADA, Parecer n.º 357/2021, Processo n.º 752/2021, 16 de dezembro de 2021.
CADA, Parecer n.º 322/2021, Processo n.º 446/2021, 10 de novembro de 2021.
CADA, Parecer n.º 260/2021, Processo n.º 564/2021, 8 de setembro de 2021.
CADA, Parecer n.º 77/2021, Processo n.º 30/2021, 24 de março de 2021.
CADA, Parecer n.º 141/2020, Processo n.º 294/2020, 14 de julho de 2020
CADA, Parecer n.º 18/2021, Processo n.º 674/2020, 20 de janeiro de 2020.
CNPD, Orientação relativa à publicação na *Internet* das atas de reuniões de órgãos colegiais, 18 de abril de 2023.

Grupo de Trabalho de Proteção de Dados do Artigo 29.º, "Parecer 4/2007 sobre o conceito de dados pessoais", 20 de junho de 2007.

8 | PRAZOS DE CONSERVAÇÃO DE DADOS PESSOAIS

*Francisco Rodrigues Rocha**

Resumo

No presente estudo, propomo-nos analisar o regime geral aplicável aos prazos de conservação de dados pessoais, constante do RGPD e, em termos não inteiramente coincidentes, da Lei n.º 58/2019. A determinação prévia e abstracta de prazos de conservação é fonte de dificuldades práticas consideráveis, com que os aplicadores têm quotidianamente de lidar. Não existindo «tabelas», «matrizes» ou, mesmo, «fórmulas mágicas» que resolvam todos os problemas que neste particular se levantam, é possível, através de uma apreciação crítica, ensaiar vias de explicação e de (tentar) pôr em prática o regime vigente.

Palavras-chave

dados pessoais – limitação das finalidades – minimização dos dados – limitação da conservação – prazos de conservação – prazos de exercício de direitos.

Sumário

* Professor Auxiliar Convidado da Faculdade de Direito de Lisboa. Advogado.

O presente texto retoma, no essencial, a nossa anotação ao artigo 21.º da LE no *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, coord. A. Barreto Menezes Cordeiro, Almedina, Coimbra, 2021, 600-606, com desenvolvimentos de conteúdo, fruto de reflexões posteriores, e decorrentes da diferente natureza e contexto de um e doutro escrito.

(263) Não sendo abundante a bibliografia sobre a matéria, destacamos, *colorandi causa*, na literatura nacional, A. Barreto Menezes Cordeiro, *Direito da Proteção de Dados*, 160, Alexandre Sousa Pinheiro/Carlos Jorge Gonçalves, anotação ao artigo 5.º, no *Comentário ao Regulamento Geral de Proteção de Dados*, coord. Alexandre Sousa Pinheiro, Almedina, Coimbra, 2018, 211-212, Francisco Rodrigues Rocha, anotação ao artigo 21.º, no *Comentário ao Regulamento Geral de Proteção de Dados* cit., 600-606, Graça Canto Moniz, *Manual de introdução à proteção de dados*, Almedina, Coimbra, 2023, 118-122; no domínio específico do direito laboral, Duarte Abrunhosa e Sousa/Rui Coimbra Gonçalves, *Cessação do contrato de trabalho e conservação de dados pessoais dos trabalhadores*, n'O *Regulamento Geral de Proteção de Dados e as relações de trabalho. Estudos APoDiT 6*, coord. Maria do Rosário Palma Ramalho/Teresa Coelho Moreira, AAFDL, Lisboa, 2020, 197-224, ou Patrícia Batista Santos, *A (possível) limitação legal no prazo de conservação dos dados pessoais dos candidatos a emprego, no Anuário da Proteção de Dados* (2020), 121-137.

(264) Por ex., uma empresa que pretenda, em documento interno, elaborar uma tabela de uso pelos seus colaboradores, em que sejam previstos todos os prazos de conservação possíveis, constatará de forma penosa, se pensar detidamente no problema, que um tal exercício pretensamente exauriente mostrará que o universo de situações é praticamente inesgotável. Uma pessoa colectiva pode praticar uma miríade de actos dentro, mas também fora do seu objecto social (na medida em que tenha capacidade de gozo para tanto) que levem à produção de documentos e ao tratamento de dados pessoais e em relação aos quais não é possível prever com exactidão todos os prazos. De resto, em relação a um mesmo dado pessoal, que seja necessário à prova de mais de um direito, podem correr, em simultâneo, diferentes prazos de conservação (por ex., para efeitos contra-ordenacionais, para efeitos tributários ou para efeitos de prova e exercício de direitos emergentes de relações contratuais). Parece-nos, sim, possível a elaboração de tabelas contendo prazos que se tenham por representativos para a actividade de uma empresa, sem precludir naturalmente a existência de outros.

(265) Com excepção do Regulamento aprovado pela Portaria n.º 112/2023 – com um âmbito de aplicação, todavia, relativamente circunscrito –, que fixa prazos de conservação, *rectius* deveres de conservação durante certo prazo, de cumprimento «obrigatório» (artigo 9.º/2), mesmo que os suportes em causa não contenham dados pessoais.

1. Introdução

I. Tema que, na prática, muitas dúvidas suscita, a determinação dos prazos de conservação de dados pessoais constitui também um campo interessante, dentro do direito da protecção de dados (pessoais), para um excurso dogmático-jurídico[263].

Sucedia e sucede, com frequência, os dados pessoais serem, por inércia ou por cautela do responsável pelo tratamento contra uma qualquer eventualidade futura, guardados indefinidamente. Situações deste género podem trazer prejuízo aos seus titulares, ficando expostos por períodos prolongados, muito superiores àqueles que seriam necessários para o tratamento dos dados de acordo com as finalidades da sua recolha.

O RGPD, como já antes a DPDP e a LPDP II, combate este estado de coisas, impondo certa previsibilidade dos prazos de conservação no momento da sua recolha e a cessação do seu tratamento terminadas as finalidades que presidiram à sua obtenção. Como princípio, esta linha de raciocínio parece incontestável. O problema reside, porém, na forma como os responsáveis pelo tratamento e subcontratantes ponham tais regras em prática[264]. Como se encontra redigido, fornece o RGPD sobretudo critérios gerais, por isso mesmo de difícil concretização. A LE, apesar das críticas que, neste tocante, lhe foram movidas, torna o RGPD mais exequível, mas, ainda assim, como veremos, dúvidas várias não deixam de se levantar e novos problemas acabaram por ser criados.

II. Impõe-se, antes de avançarmos, que exaremos algumas ressalvas de ordem geral.

Escrevemos sobre prazos de conservação, repetimos, de *dados pessoais* – informação relativa a uma pessoa singular identificada ou identificável por referência a um identificador ou a um ou mais elementos específicos da sua identidade (artigo 4.º/*1*) do RGPD) –, não genericamente sobre (prazos de) conservação de *dados,* que é conceito muito mais abrangente. A lei impõe, imperativamente, prazos de conservação e, consequentemente, de eliminação somente aos *dados pessoais*[265].

Escrevemos também sobre *dados (pessoais),* não sobretudo ou apenas sobre *documentos* («pessoais»). *Documento* é qualquer objecto elaborado pelo homem com o fim de reproduzir ou representar uma pessoa, coisa ou facto (cf. o artigo 362.º do CC); mediante documentos produz prova de factos *(prova documental).* Um ou mais dados pessoais podem estar contidos num documento; diremos, até, que os dados pessoais estarão, via de regra, contidos em documentos, dado a pura memorização dos mesmos não parecer abrangida pelo RGPD. Mas – observação óbvia que, todavia, convém ser lembrada – um documento normalmente, quando contém dados pessoais, contém também dados não pessoais; já para não falar da multitude de documentos que contém apenas dados não pessoais. Mais: um documento digamos compósito, por exemplo por múltiplas páginas, pode conter e normalmente contém partes com dados pessoais – outras, até, com dados pessoais qualificados, como os sensíveis – e outras sem tais dados. Ora, repetimos, a lei impõe prazos de conservação somente aos *dados pessoais* ou, doutra perspectiva, dentre a muita que um documento compreenda, somente a informação que constitua *dados pessoais.* Nos casos em que os documentos não contenham dados pessoais ou nos casos em que os contenham mas sejam tais dados eliminados ou despersonificados (anonimização, pseudonimização), preservando-se o restante conteúdo do documento, os documentos poderão ser, em princípio, conservados sem limite temporal. O mesmo vale para as partes dos documentos que não contenham dados pessoais: sendo destacável a parte que os contenha, o documento pode manter-se com a parte que incorpore informação não personalizada ou personalizável.

O discurso subsequente considera, *prima facie,* prazos de conservação de *dados pessoais* e tem em conta apenas os *documentos* que os contenham. A arquivística ou o tema, em voga, da «*gestão da informação*», incluindo a classificação e avaliação de documentos e informação neles contida, é mais abrangente do que a protecção de dados e concita problemáticas não coincidentes. Um exemplo pode encontrar-se no recém-aprovado Regulamento para a Classificação e Avaliação da Informação Arquivística da

Administração Local, aprovado pela Portaria n.º 112/2023, de 27 de Abril[266]. Trata-se de um diploma que, sintomaticamente, alude apenas uma vez a «dados pessoais», numa das linhas[267] da ingente tabela que consta do anexo I. A tónica é colocada sobre a *«informação arquivística»* (artigo 1.º/1) e na *«gestão de informação»* (capítulo II, artigos 5.º ss.)[268]. Trata-se, pois, de informação que não tem de conter dados pessoais: quando seja o caso, a lógica do RGPD impera e, interpretada em conformidade com este, a da LE, ambos fontes normativas hierarquicamente superiores a uma portaria. Note-se, porém que, também num domínio no qual não têm forçosamente de existir dados pessoais, existe a preocupação de definir *«prazos de conservação administrativa»* (artigo 3.º *x*))[269], de «cumprimento (...) obrigatório» conforme determinado na tabela de selecção constante do anexo I (artigo 9.º/2[270], conjugado com o 3.º *dd)* e 7.º/1), bem como a respectiva *«forma de contagem»* (artigos 3.º *q*)[271] e 10.º). A rigidez e pretensão de exaustividade deste Regulamento conjugam-se

---

[266] Cuja revisão fora já sugerida, em sede de trabalhos preparatórios da LE, a propósito do artigo 21.º/1, pela pronúncia da ANMP, de 15-mai.-2018. A matéria era então regulada pelo Regulamento Arquivístico para as Autarquias Locais, aprovado, à data, pela Portaria n.º 412/2001, de 17-Abr., alterado pela Portaria n.º 1253/2009, de 14-Out.

[267] Correspondente ao código 650.20.604, título «Processamento de dados cadastrais de utentes em respostas sociais de acolhimento».

[268] Outro exemplo: a Norma ISO 27001, sobre Sistemas de Gestão da Segurança da Informação (última versão de 2022).

[269] Além das dificuldades hermenêuticas enunciadas na nt. seguinte, compreende-se mal que tais prazos se refiram apenas ao «período de tempo, em *anos*». A especificação dos fins é também atabalhoada e (juridicamente) imprecisa: «para responder às necessidades de negócio, requisitos organizacionais, responsabilização e obrigações legais, previsto na tabela de seleção».

[270] Dogmaticamente parece-nos errado o artigo 9.º/4: «A contagem do prazo de conservação administrativa suspende-se sempre que for instaurado procedimento que requeira o uso dos documentos e agregações para obtenção de prova de infração ou ilícito, caso em que os prazos de conservação passam a ser os previstos na lei para cuja aplicação a informação é utilizada». Do que se trata não é de *suspensão* do prazo ou, como diz a lei, de contagem do prazo (linguagem de resto típica do direito sancionatório, em que possivelmente se estava a pensar), mas de uma *prorrogação do prazo* de conservação inicialmente previsto de acordo com um fim ulterior. A referência a «lei para cuja aplicação a informação é utilizada» suscita também dificuldades interpretativas: o pronome «cuja» significa «da lei»; ora, a ser assim este segmento significa «lei para cuja [= da lei] aplicação a informação é utilizada» ou «lei para (...) aplicação da qual a informação é utilizada». Não conhecemos, possivelmente por inépcia nossa, prazos de conservação (em sentido próprio) previstos em lei que exija, para a aplicação da mesma lei (mas talvez sim finalidades aí previstas em específicas normas), que uma informação seja utilizada. A redacção é gongórica e, novamente, pouco rigorosa.

mal com a maleabilidade dos prazos de conservação e a casuística que a sua aplicação sempre implica. Poderia, em todo o caso, argumentar-se que de prazos de conservação de dados pessoais nem sempre se tratará. É verdade. Contudo, também o conceito de dado pessoal é a tal ponto abrangente que facilmente documentos administrativos conterão dados pessoais (ditos comuns); ou até mesmo dados sensíveis, sobretudo se se tiver em conta que o RGPD admite os chamados *Ausgangsdaten* (artigo 9.º/1: «dados pessoais que revelem (...)»).

III. O nosso estudo encontra-se erigido em torno dos dois principais diplomas nesta matéria: o RGDP 2016 e a LE 2019. Assim, trataremos, numa primeira parte, do regime geral constante do RGPD (2.) e, numa segunda grande parte, do regime constante do artigo 21.º da LE (3.). Dentro desta, analisaremos, sucessivamente, a regra principal nesta matéria (2.1.), a fixação de prazos de conservação por norma legal ou regulamentar (2.2.), a conservação pelo prazo de prescrição dos direitos correspondentes a deveres do responsável (2.3.), o tratamento para fins de arquivo de interesse público, investigação científica ou histórica, ou estatísticos, com uma breve incursão pelo novel Regulamento aprovado pela Portaria n.º 112/2023 (2.4.), terminando com o direito ao apagamento (2.5.) e com os dados relativos a declarações contributivas para efeito de aposentação ou reforma (2.6.).

---

(271) A definição não é boa. A al. *q)* define o conceito de «forma de contagem do prazo» como «o momento a partir do qual é iniciada a contagem do prazo de conservação administrativa». Ora, não se trata então da forma de contagem, mas do *início da contagem*, comummente conhecido por *dies a quo*. A «forma de contagem» compreende o *dies a quo*, o *dies ad quem*, a contagem propriamente dita, i.e. se em dias corridos, se contínuos, etc. As várias subalíneas em que se decompõe a al. *q)* também se sujeitam a críticas. Desde logo, não se percebe a necessidade de uma subalínea como a *i)*, que define redundantemente a expressão «Conforme disposição legal» como o caso em que «o momento em que se inicia a contagem é determinado por lei». Pergunta-se: qual prazo determinado por lei? O do prazo de conservação *administrativa*. Mas, então, o adjectivo «administrativa», na alínea *q)*, como na alínea *x)* do artigo 3.º, é, logo, fonte de outro problema: só os prazos de conservação *administrativa*? Se estiver definido por lei um prazo que não seja apenas de conservação «administrativa», não se considera para este efeito? A subalínea *iii)* define «data de *emissão* do título» como o caso em que o «momento em que se inicia a contagem é determinado pela *produção* do documento de validação ou reconhecimento»: mas então não deveria ser a data de produção do título? É que emissão e produção não são manifestamente a mesma coisa. A subalínea *vi)* alude, sem rigor técnico, a «registo do fim da entidade», na qual inclui «pessoas, empresas, bens e atividades»... Enfim, uma multiplicidade de problemas.

2. O regime geral do RGPD

I. O RGPD não é propriamente muito claro em matéria de prazos de conservação de dados. Dito doutro modo: o RGPD determina genericamente uma limitação da conservação, com manifestações específicas e pontuais noutras regras, mas concretiza pouco o modo como proceder, em concreto, na fixação de um prazo de conservação.

Ainda assim, uma análise mais minuciosa do teor e da lógica subjacente ao RGPD talvez consinta avançar um pouco na sua compreensão.

II. A regra fundamental, derivada do princípio da *limitação da conservação,* exteriorizada pelo artigo 5.º/1 *e)* do RGPD[272], é a de que os dados pessoais[273] podem ser tratados[274] *apenas* pelo prazo *necessário* aos fins do tratamento[275].

---

[272] Cf. sobre o preceito, entre nós, A. Barreto Menezes Cordeiro, anotação ao artigo 5.º, em *Comentário ao Regulamento Geral de Proteção de Dados* cit., 102-107. Noutro âmbito, vd. os artigos 4.º/1 *e)* e 5.º da Diretriz n.º 2016/680, este último, epigrafado «Prazos para a conservação e avaliação», com o seguinte teor: «Os Estados-Membros preveem prazos adequados para o apagamento dos dados pessoais ou para a avaliação periódica da necessidade de os conservar. Devem ser previstas regras processuais que garantam o cumprimento desses prazos». Em transposição da citada Directriz, o artigo 12.º da Lei n.º 59/2019, de 8-Ag., respeitante ao tratamento de dados pessoais para prevenção, detecção, investigação ou repressão de infracções penais ou execução de sanções penais (diploma, no entanto, fora das nossas imediatas preocupações no discurso subsequente). O princípio de limitação da conservação era já previsto na DPDP 1995, embora sejam agora os responsáveis pelo tratamento exortados a estabelecer limites de conservação ou prazos para revisão periódica (Cécile de Terwangne, anotação ao artigo 5.º, em *The EU General Data Protection Regulation (GDPR). A Commentary,* coord. Christopher Kuner/Lee A. Bygrave/Christopher Docksey, OUP, Oxónia, 2020, 318) – curiosamente, porém, não previa a LPDP II 1998, em transposição da DPDP 1995, qualquer norma similar ao artigo 21.º.

[273] Se não forem identificáveis ou, noutros termos, determináveis (por ex. por pseudonimização ou anonimização) as pessoas, não são dados pessoais e a questão da conservação não se coloca. Vd. também Roßnagel, anotação ao artigo 5.º, em *Datenschutzrecht. DSGVO mit BDSG,* coord. Spiros Simitis/Gerrit Hornung/Indra Spiecker, Nomos, Baden-Baden, 2019, 392.

[274] No tratamento inclui-se a conservação (artigo 4.º/2 do RGPD); a mera conservação, seja com ou sem uso dos dados, é sempre tratamento. Há um jogo de palavras, de certa perspectiva e em parte redundante, na 1.ª prt. do artigo 5.º/1 *e)* do RGPD: «Os dados pessoais são: conservados [= tratados, ainda que o tratamento não se circunscreva à conservação] (...) durante o período necessário às finalidades para as quais são tratados». O (parcial) pleonasmo continua na segunda parte do preceito: «os dados pessoais podem ser conservados [= tratados, posto que o tratamento à conservação se não cinja] (...), desde que tratados (...)».

[275] Cf. o considerando 39: «é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. (...) A fim de assegurar que os dados pessoais sejam conservados apenas durante o período necessário o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica». Na jurisprudência, vd. TJUE 13-Mai.-2014 (*Google Spain SL/Google Inc. v. Agencia Española de Protección de Datos/Mario Costeja González),* proc. n.º C-131/12 (ECLI:EU:C:2014:317), §§ 92-95. Em consequência: exaustos os fins, devem os dados deixar de ser tratados, o que significa, na prática, deverem ser, sem injustificada demora (artigo 17.º/1 do RGPD; artigo 21.º/4 não estabelece um prazo), eliminados ou anonimizados (artigo 21.º/4 da LE; o artigo 5.º/1 *e)* do RGPD não fornece resposta imediata, senão *a contrario sensu*). Vd. também Roßnagel, anotação ao artigo 5.º, em *Datenschutzrecht* cit., 392-393.

O teor do citado preceito é o seguinte:

> «*e)* Os dados pessoais são: (...) conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»)».

Directamente relacionado com este preceito está o considerando 39:

> «Os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. Os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica. Deverão ser adotadas todas as medidas razoáveis para que os dados pessoais inexatos sejam retificados ou apagados».

Interessa-nos, de momento, a primeira parte da alínea *e)*. Através da regra nela contida evita-se a sujeição do titular dos dados ao tratamento *eterno* destes[276]. O prazo está directamente dependente dos fins do tratamento: a ideia de circunscrição cronológica do tratamento cruza com a dos fins (princípio da *limitação das finalidades*[277]), que devem também ser o mais

---

[276] Vd. expressivamente C. de Terwangne, *Les principes relatifs au traitement des données à caractère personnel et à sa licéité,* em *Le Règlement Général sur la Protection des Données* (RGPD/*GDPR*). *Analyse approfondie,* coord. C. de Terwangne/Karen Rosier, prefácio de Yves Poullet, 113-114: «Il n'est pas légitime de conserver, pour la plupart des traitements de données, *ad vitam aeternam* les données sous une forme permettant l'identification des personnes».

[277] Vd. Pötters, anotação ao artigo 5.º, em *DS-GVO. Datenschutz-Grundverordnung VO (EU) 2016/679. Kommentar,* coord. Peter Gola, 2.ª ed., Beck, Munique, 2018, 222, Frenzel, anotação ao artigo 5.º, em *Datenschutz-Grundverordnung Bundesdatenschutzgesetz,* coord. Boris P. Paal/Daniel A. Pauly, 2.ª ed., Beck, Munique, 2018, 82, ou Herbst, anotação ao artigo 5.º, em *Datenschutz-Grundverordnung. Bundesdatenschutzgesetz. Kommentar,* coord. Jürgen Kühling/Benedikt Buchner, 2.ª ed., Beck, Munique, 2018, 229. A proximidade da limitação das finalidades à da conservação manifesta-se inclusive na segunda parte das als. *b)* e *e)* do n.º 1 do artigo 5.º do RGPD: em ambas existe a preocupação de exceptuar o tratamento para fins de arquivo de interesse público, investigação científica ou histórica e estatísticos.

possível circunscritos[278]. A ideia de limitação da conservação resulta do mais amplo *princípio da proporcionalidade*[279] e é, ainda, geminada ao da *minimização dos dados*[280-281] (artigo 5.º/1 *c)*).

---

[278] Aliás, quanto mais limitadas as finalidades, mais fácil a determinação do prazo máximo de conservação. Assim, Roßnagel, anotação ao artigo 5.º, em *Datenschutzrecht* cit., 379.

[279] Assim, a Deliberação da CNPD n.º 1039/2017, de 27-Jul., proc. n.º 7166/2010, fl. 5v. («de acordo com o princípio da proporcionalidade, concretizado nas alíneas *c)* e *e)* do artigo 5.º da LPDP»); na doutrina, Roßnagel, anotação ao artigo 5.º, em *Datenschutzrecht* cit., 392, Pötters, anotação ao artigo 5.º do RGPD, em *DS-GVO Kommentar* cit., 222, entre nós, Nuno Pinto Oliveira, *A declaração de consentimento pré-formulada. Articulação entre a Directiva 1993/13/CEE, de 5 de Abril de 1993,* e o *Regulamento 2016/679/UE, de 27 de Abril de 2016, BBS* 3 (2018), 17 (assinalando a semelhança entre o controlo dos meios através dos princípios da adequação e da necessidade implicitamente exigido no artigo 3.º da Directiva n.º 1993/13/CEE e os princípios da minimização dos dados e da limitação da conservação consagrados no artigo 5.º/1 *c)* e *e)* do RGPD). Vd. também, na jurisprudência constitucional, *e. g.* TC n.º 527/95, de 4-Out. (s/ indicação de relator; voto vencido de Bravo Serra), proc. n.º 152/95, TC n.º 187/2001, de 2-Mai. (Paulo Mota Pinto; votos vencidos de Guilherme da Fonseca e Maria Helena Brito), proc. n.º 120/95, TC n.º 632/2008, de 23-Dez. (s/ indicação de relator), proc. n.º 977/2008.

[280] Considera que o princípio da limitação da conservação concretiza o da minimização Heberlein, anotação ao artigo 5.º, em *Datenschutz-Grundverordnung,* Eugen Ehmann/Martin Selmayr, 2.ª ed., Beck, Munique, 2018, 199. Com Roßnagel, anotação ao artigo 5.º, em *Datenschutzrecht* cit., 392, diremos que ambos derivam do princípio da proporcionalidade ou necessidade, tendo «objectos» diversos: o da minimização os próprios dados e o seu tratamento, o da limitação da conservação a duração do tratamento.

[281] Buchholtz/Stentzel, anotação ao artigo 5.º, em *Kommentar Datenschutz-Grundverordnung*, coord. Sibylle Gierschmann/Katharina Schlender/Rainer Stentzel/Winfried Veil, Bundesanzeiger, Colónia, 2018, 190, ligam o princípio da limitação da conservação também ao da exactidão (artigo 5.º/1 *e)*), em termos que não acompanhamos, ainda que compreendamos por que o afirmam em face do teor literal do artigo 5.º/1 *e)*: «conservados de uma forma que» em vez de «conservados de forma [a] que» (vd. também as versões alemã: «in einer Form gespeichert werden, die»; inglesa: «kept in a form which»; francesa: «conservées sous une forme permettant», italiana: «conservati in una forma che»; holandesa: «worden bewaard in een vorm die»; algo diversamente, a castelhana, em que o pronome relativo «que» introduz uma oração subordinada completiva ou integrante e o sujeito da forma apassivada «se permita» é «la identificación»: «mantenidos de forma que se permita la identificación de los interesados durante no más tiempo»); não era assim na versão do artigo 5.º *e)* da CTADP 1981 («Conservados de forma [a] que permitam»), nem na do artigo 6.º/1 *e)* da DPDP («Conservados de forma a permitir»), nem no artigo 5.º/1 *e)* da LPDP I («Conservados de forma a»), onde se optava por uma oração subordinada final e a forma verbal do verbo desta oração concordava com «dados», que não com «forma». As matizes semânticas são num caso e noutro ligeiras (até porque, na versão do RGPD, o conjuntivo da oração relativa também lhe confere uma «coloração» final), posto que não despiciendas. De todo o modo, duma perspectiva puramente literal, o foco incide agora sobre a «forma» em que são conservados os dados e no facto de permitir ela a identificação dos seus titulares (vd. também Roßnagel, anotação ao artigo 5.º, em *Datenschutzrecht* cit., 392), ao passo que antes incidia sobre «conservados», ou seja, sobre a sua conservação, tida como forma de permitir a identificação dos referidos titulares.

O RGPD concretizou o princípio da limitação da conservação, desde logo, na fixação dum critério geral (limitação da duração pelos fins: artigo 5.º/1 *e)*)[282], mas também, mais em específico:

(i) na imposição ao responsável pelo tratamento do dever de fixar um prazo (determinado) ou, caso não seja possível, ao menos a enunciação dos critérios para a sua fixação (prazo indeterminado mas determinável) (artigos 13.º/2 *a)* e 14.º/2 *a)* ou 15.º/1 *d)* do RGPD);

(ii) no direito ao apagamento (artigo 17.º/1 *a)* do RGPD);

(iii) no direito à limitação (artigo 18.º/1 do RGPD);

(iv) no dever de registo dos prazos de conservação (artigo 30.º/1 *f)* do RGPD); ou, mesmo;

(v) em matéria de *privacy by default* (artigo 25.º/2)[283].

Contudo, não estabelece o RGPD, mais em particular, prazos em concreto para o efeito. A este nível, a LE – ainda que não incontestadamente – pode ser mais prestável.

3. O artigo 21.º da LE

I. Exposto o regime do RGPD, passemos à LE.

A *sedes materiae* está no artigo 21.º, cuja redacção importa recordar.

---

(282) A natureza sensível ou especial do dado pessoal em questão parece, olhando para o artigo 5.º/1 *e)* do RGPD, não ter importância. Como princípio, porém, atenta a proibição de base do n.º 1 do artigo 9.º *ibid.*, uma tal natureza deve ser tida em conta, impondo, à partida, que o prazo de conservação seja menor.

(283) Pondo em prática mecanismos técnicos que prevejam, ultrapassado certo prazo, o término automático da conservação: cf. Francisco Rodrigues Rocha, anotação ao artigo 25.º, em *Comentário ao Regulamento Geral de Proteção de Dados* cit., 239-244. C. de Terwangne, *Les principes relatifs au traitement* cit., 114, dá como exemplo a implementação de sistemas automáticos de eliminação de dados como o X-Pire, lançado na Alemanha, que permite aos utilizadores inserir uma data de termo às imagens publicadas em redes sociais como o *Facebook* desde que sejam adotadas medidas técnicas organizativas adequadas a garantir os direitos do titular dos dados.

Artigo 21.º
Prazo de conservação de dados pessoais

1 – O prazo de conservação de dados pessoais é o que estiver fixado por norma legal ou regulamentar ou, na falta desta, o que se revele necessário para a prossecução da finalidade.

2 – Quando, pela natureza e finalidade do tratamento, designadamente para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos, não seja possível determinar antecipadamente o momento em que o mesmo deixa de ser necessário, é lícita a conservação dos dados pessoais, desde que sejam adotadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados, designadamente a informação da sua conservação.

3 – Quando os dados pessoais sejam necessários para o responsável pelo tratamento, ou o subcontratante, comprovar o cumprimento de obrigações contratuais ou de outra natureza, os mesmos podem ser conservados enquanto não decorrer o prazo de prescrição dos direitos correspetivos.

4 – Quando cesse a finalidade que motivou o tratamento, inicial ou posterior, de dados pessoais, o responsável pelo tratamento deve proceder à sua destruição ou anonimização.

5 – Nos casos em que existe um prazo de conservação de dados imposto por lei, só pode ser exercido o direito ao apagamento previsto no artigo 17.º do RGPD findo esse prazo.

6 – Os dados relativos a declarações contributivas para efeitos de aposentação ou reforma podem ser conservados sem limite de prazo, a fim de auxiliar o titular na reconstituição das carreiras contributivas, desde que sejam adotadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados.

II. O artigo 21.º da Proposta de Lei, que deu origem à LE, era largamente coincidente com aquela que veio a ser a sua redacção final, exceptuadas duas alterações e um aditamento (o n.º 6):

(i) não era prevista a adopção de medidas técnicas e organizativas adequadas no n.º 2;

(ii) não eram especificados os tipos de obrigações em causa no n.º 3 («contratuais ou de outra natureza»); e

(iii) não constava do artigo aquele que veio posteriormente a ser o n.º 6 (dados relativos a declarações contributivas para efeito de aposentação ou reforma).

III. Muito crítica deste preceito foi a CNPD. Para esta autoridade[284], no Parecer n.º 20/2018, de 2 de Maio[285], merecia o artigo 21.º «vigoroso reparo», em razão de um conjunto de argumentos:

(i) não especificar que por prazos de conservação se visavam os «prazos máximos de conservação»;

(ii) o RGPD só admitir aos Estados-membros legislar sobre a matéria quanto à conservação de dados durante períodos mais longos, quando em causa a prossecução exclusiva de fins de arquivo de interesse público, de investigação científica, histórica ou estatísticos;

(iii) os n.os 1 e 4 «subverte[re]m o princípio da limitação da conservação com assomos de repetição ademais incorreta do direito da União»;

(iv) o n.º 3 introduzir uma finalidade autónoma e genérica comum a todos os tratamentos e paralela às finalidades de cada um deles, «para dar cobertura a uma conservação de dados por tempo quase ilimitado, o que é verdadeiramente intolerável», sem que a comprovação do cumprimento fosse uma finalidade em si mesma e abrangendo os subcontratantes que não tinham na sua disponibilidade estabelecer tais prazos;

(v) o n.º 5 opor-se «manifestamente» ao artigo 17.º do RGPD, pois «não é o facto de existir um prazo de conservação de dados, legalmente fixado, que poderá ser impeditivo de o titular dos dados exercer o seu direito ao apagamento», não existindo relação entre os dois vectores, «sendo o n.º 5 contrário ao RGPD ao pretender coarctar o exercício de um direito por motivo não atendível de acordo com o regulamento europeu»;

---

(284) Além do Parecer da CNPD, outros houve, ainda que de menor importância. Pensamos por exemplo na pronúncia da ANMP de 15-mai.-2018 que, na senda do artigo 21.º/1, sugeriu a revisão do Regulamento Arquivístico para as Autarquias Locais, aprovado, à data, pela Portaria n.º 412/2001, de 17-Abr., alterado pela Portaria n.º 1253/2009, de 14-Out.

(285) proc. n.º 6275/2018, 11-12v.

(vi) o n.º 2 «causa[r] a maior perplexidade», ao «dispensar a limitação da conservação dos dados (…) com uma tal amplitude», pois, «tal como está redigida, a norma permite a conservação ilimitada de dados pessoais *para qualquer finalidade,* por consideração ainda de um fator que não vem considerado no RGPD» (a natureza do tratamento), e ser omisso quanto à adopção de medidas técnicas e organizativas mencionadas no artigo 5.º/1 *e)* do RGPD, de modo que violava o princípio da proporcionalidade e os artigos 5.º/1 *e)* e 89.º/1 do RGPD.

Nas conclusões do seu parecer e na proposta de articulado, a CNPD propunha a eliminação do artigo 21.º, com excepção do n.º 2, que, entendia, «dev[ia] ser revisto». Contudo, o artigo 21.º não viria a constar do elenco de normas cuja desaplicação, por manifesta incompatibilidade com o direito da UE, a CNPD verberou através da Deliberação 2019/494, de 3 de Setembro.

3.1 Fixação de prazos de conservação por norma legal ou regulamentar

I. O artigo 21.º/1 da LE fornece, como primeiro critério, a fixação legal ou regulamentar de prazos de conservação.

Vimos já não ser essa a regra fundamental do direito da UE no artigo 5.º/1 *e)*, que ao artigo 21.º/1 se sobrepõe[286]. Os prazos legais ou regulamentares de conservação não constituem em si mesmos um fim[287], mas podem ser um fundamento do tratamento, de modo que, onde a lei os estabeleça, é possível, com base neles, fundar o *tratamento ulterior* para fins que não os da recolha[288] e apenas os conformes a tais fins (artigo 6.º/*4*: «com base (…) em

[286] Assim também da CNPD o Parecer n.º 20/2018 cit., 11 ss.

[287] Parecer da CNPD n.º 20/2018 cit., 11 ss., ainda que a 11v. afirme que: «[a] aplicação deste princípio [da limitação da conservação] não prejudica, obviamente, a necessidade de conservar dados quando haja lei que a tal obrigue».

[288] No Parecer 20/2018 da CNPD encontramos um exemplo: «um tratamento de dados de gestão de clientes, em que é obrigatória a empresa manter os dados de faturação do cliente por um período de 10 anos para fins fiscais, não decorrendo o dever de conservar outros dados relativos ao cliente (tais como contactos, idade, consumos detalhados, interesses e preferências) se a relação contratual for terminada ao fim de dois anos».

disposições do direito (...) 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»).

A referência a prazos estabelecidos por regulamento pode suscitar problemas, parecendo-nos delicado considerar como norma habilitante, para tal efeito, o tão abrangente n.º 1 do artigo 21.º da LE.

II. Dos *prazos de conservação* de dados pessoais devemos distinguir os *prazos de exercício de direitos* para cuja prova sejam necessários dados pessoais[289]. Os primeiros visam constituir na esfera do destinatário da norma um *dever legal,* via de regra sancionado a nível contra-ordenacional, de conservação dos dados durante certo lapso temporal; os segundos visam definir temporalmente situações jurídicas, sancionando a inércia do titular ou promovendo a certeza e segurança jurídicas, ao determinar a modificação ou a extinção do direito.

Contrariamente ao que pudesse pensar-se, não é muito frequente que a lei estabeleça prazos de conservação de dados pessoais. Por isso se apresenta tão importante o subsídio que os prazos de exercício de direitos – que todos têm, mais não seja pela regra geral que do artigo 309.º do CC consta (20 anos) – prestem à determinação de prazos de conservação.

III. Não fazemos tenções, nem temos sequer a veleidade de elencar aqui todos os dados de conservação de dados pessoais existentes no ordenamento jurídico português, senão apenas alguns que por representativos temos. Assim:

(i) o artigo 40.º/1 do CCom: «Todo o comerciante é obrigado a arquivar a correspondência emitida e recebida, a sua escrituração mercantil e os documentos a ela relativos, devendo conservar tudo pelo *período de 10 anos*» (o prazo encontra-se dobrado, em termos a articular, com os previstos no artigo 130.º/1 do Código do IRC, aprovado pelo

[289] E sobre os quais falaremos dentro em pouco infra, secção 2.3.

Decreto-Lei n.º 442-B/88, de 30 de Novembro[290], e com o artigo 52.º/1 do Código do IVA, aprovado pelo Decreto-Lei n.º 102/2008, de 20 de Junho);

(ii) artigo 52.º/1 do CIVA: «Os sujeitos passivos são obrigados a arquivar e conservar em boa ordem *durante 10 anos civis subsequentes* todos os livros, registos e respectivos documentos de suporte, incluindo, quando a contabilidade é estabelecida por meios informáticos, os relativos à análise, programação e execução dos tratamentos»;

(iii) artigo 51.º da Lei n.º 83/2017, de 18 de Agosto, em matéria de luta contra o branqueamento de capitais e financiamento do terrorismo: «As entidades obrigadas conservam, por um *período de sete anos* após o momento em que a identificação do cliente se processou ou, no caso das relações de negócio, após o termo das mesmas: *a)* as cópias, registos ou dados eletrónicos, extraídos de todos os documentos que obtenham ou que lhes sejam disponibilizados pelos seus clientes ou quaisquer outras pessoas, no âmbito dos procedimentos de identificação e diligência (...)»[291];

(iv) o artigo 136.º/6 da nova Lei das Comunicações Electrónicas, aprovada pela Lei n.º 16/2022, de 16 de Agosto, estabelece que: «Qualquer suporte duradouro, incluindo gravação telefónica, relacionado com a denúncia de contratos de prestação de serviços de comunicações eletrónicas acessíveis ao público (...) deve ser conservado pelas empresas durante o prazo de *prescrição e caducidade*[292] resultantes do contrato e entregue à ARN ou ao consumidor, em suporte duradouro adequado, sempre que tal seja requerido por uma ou outro»[293];

---

(290) Cf. também o artigo 123.º para lista e organização dos documentos.

(291) *Dies a quo:* a contar do momento em que a identificação do cliente se processou ou, em caso de relações de negócio, a contar do termo das mesmas.

(292) Ambos em simultâneo? O prazo ou os prazos? A redacção da lei é, a este nível, problemática.

(293) O antecedente artigo 47.º-A/5 *a)* da Lei das Comunicações Electrónicas, aprovada pela Lei n.º 5/2004, de 10-Fev., na redacção da Lei n.º 15/2016, de 17-Jun., estabelecia: «Em relação ao contrato que estabeleça um período de fidelização, inicial ou sucessivo, as empresas referidas no n.º 1 devem: *a)* Conservar, no caso de celebração por telefone, a gravação das chamadas telefónicas *durante todo o período de vigência acordado,* inicial ou sucessivo, *acrescido do correspondente prazo de prescrição e caducidade».*

(v) artigo 6.º da Lei n.º 32/2008 epigrafado «Período de conservação»: «As entidades referidas no n.º 1 do artigo 4.º devem conservar os dados previstos no mesmo artigo pelo *período de um ano* a contar da data da conclusão da comunicação»;

(vi) o artigo 3.º/1 *d)* do Decreto-Lei n.º 156/2005, de 15 de Setembro, na redacção dada pelo Decreto-Lei n.º 74/2017, de 21 de Junho, em matéria de livro de reclamações: «O fornecedor de bens ou prestador de serviços é obrigado a: (...) manter, por um *período mínimo de três anos,* um arquivo organizado dos livros de reclamações que tenha encerrado»; (cf. também o artigo 5.º–A/3)[294];

(vii) os artigos 202.º/1 e 4 e 231.º/1 e 8 do CT para registos de tempos de trabalho e de trabalho suplementar, impondo prazo de conservação por 5 *anos*[295];

(viii) o artigo 32.º do CT para registo de processos de recrutamento, com um prazo de 5 *anos*[296];

(ix) também em sede laboral, o artigo 46.º da Lei n.º 102/2009, de 10 de Setembro, que aprovou o Regime Jurídico da Promoção da Segurança e Saúde no Trabalho, impondo um prazo de, «pelo menos», *40 anos* (prazo de conservação anormalmente longo)[297].

---

[294] A lei estabelece, algo estranhamente, um «período mínimo» de 3 anos, de maneira que, à letra, não preclude a interpretação segundo a qual possa tal livro ser preservado por período mais alargado, designadamente se permitir a prova de direitos para os quais valha um prazo de prescrição mais alargado. Fora deste quadro, é, em face do disposto no artigo 5.º/1 *e)* do RGPD, discutível que os dados possam ser conservados por períodos mais longos do que os três anos. A lei não é clara quanto ao *dies a quo* de contagem do prazo: contudo, ao aludir «livros de reclamações que tenha encerrado» está a remeter para o regime de encerramento ou conclusão do livro, ou seja, a estabelecer que o prazo deverá contar-se a partir do acto ou termo de encerramento do livro.

[295] Vd., com indicações, Duarte Abrunhosa e Sousa/Rui Coimbra Gonçalves, *Cessação do contrato de trabalho e conservação de dados pessoais dos trabalhadores,* em *O Regulamento Geral de Proteção de Dados e as relações de trabalho. Estudos APoDiT 6*, coord. Maria do Rosário Palma Ramalho/Teresa Coelho Moreira, AAFDL, Lisboa, 2020, 197-224.

[296] Constitui contra-ordenação leve a violação do disposto no artigo 32.º do CT. *Dies a quo*: a lei não determina; parece ser o do termo do processo de recrutamento.

[297] Constitui contra-ordenação grave a violação do disposto no artigo 46.º da Lei n.º 102/2009. *Dies a quo:* «pelo menos», 40 anos após ter terminado a exposição dos trabalhadores a que digam respeito. Se a empresa cessar a actividade, os registos e arquivos devem ser transferidos para o organismo competente do membro do Governo responsável pela área laboral, com excepção das fichas clínicas, que devem ser enviadas para o organismo competente do ministério responsável pela área da saúde, os quais asseguram a sua confidencialidade.

3.2. Conservação pelo prazo de prescrição dos direitos correspondentes a obrigações do responsável

I. O n.º 3 do artigo 21.º da LE[298] permite genericamente a conservação de dados pessoais necessários à prova do «cumprimento de obrigações contratuais ou de outra natureza [entenda-se: legal[299]]» «enquanto não decorrer o prazo de prescrição dos direitos correspetivos».

A referência no artigo 21.º/3 apenas a *prazos de prescrição* não se compreende, senão por má técnica legislativa: obviamente, podem estar também em causa *prazos de caducidade* – que o legislador, de certo modo, erige em regra supletiva (artigo 298.º/2 do CC; ainda que no 298.º/1 tenha a prescrição por regra geral) –, sem que se divisem razões minimamente atendíveis para os excluir[300].

A previsão normativa de *prazos de exercício de direitos* é, como acima consignámos, situação mais frequente – e genérica ou residual – do que a de prazos de conservação. Na prática, portanto, a determinação dos *prazos de conservação* far-se-á por recurso àqueles. Claro está que, mesmo assim, nem sempre será fácil determinar um concreto prazo de conservação: mais uma vez, sobre um certo dado pessoal podem incidir um ou mais prazos de exercício de direitos, logo de conservação; a lei nem sempre ajuda à determinação do *dies a quo* ou, mesmo quando o faz, o apuramento das circunstâncias fácticas que o iniciam não é simples; também em caso de transmissão do crédito, por ex. por sub-rogação, no campo da responsabilidade delitual, persistem dúvidas apreciáveis sobre se continue a correr o prazo inicial (artigos 585.º e 308.º/1 do CC), se deva recomeçar a sua contagem à data da transmissão (artigo 498.º/2 do CC); outrossim na hipótese de direito de regresso, nas obrigações solidárias, haverá que contar novo prazo a contar do cumprimento (artigo 498.º/2 do CC).

---

[298] Que com o n.º 1 se relaciona, da perspectiva segundo a qual o n.º 3 transformaria os prazos de prescrição em prazos de conservação. Como exarado em texto, não é exactamente assim.

[299] Quando legais os deveres, talvez seja preferível falar, com maior rigor conceptual, de *deveres,* em lugar de *obrigações* (para estas, cf. os artigos 397.º e 398.º/2 do CC). *Ex multis,* Antunes Varela, *Das obrigações em geral,* vol. I, 10.ª ed., Coimbra, Almedina, 54-62.

[300] Uma forma mais neutra de expressão teria sido: «prazos de exercício dos direitos correspectivos».

II. Como notou a CNPD, «o prazo de conservação de dados está sempre adstrito à finalidade específica do tratamento que esteve na base da sua recolha ou tratamento posterior», de modo que, via de regra, a conservação, para efeitos probatórios[301], constituirá uma *finalidade ulterior compatível,* com base no direito nacional (cf. o artigo 6.º/4 do RGPD)[302]. Em todo o caso, o RGPD permite também o *cúmulo de finalidades,* inclusive logo no momento inicial da recolha, e, desta forma, a possibilidade de conservação de dados sujeita ao decurso de diferentes prazos de conservação[303].

Fossem, para efeito da determinação de prazos de conservação dos dados pessoais, irrelevantes os prazos de prescrição e caducidade – o que, como resulta da posição que assumimos e algo diversamente da CNPD, nos não parece o caso –, haveria que trazer a terreiro a aplicação ou não de regras de *inversão do ónus da prova* (difícil e excepcionalmente os artigos 344.º/2 do CC e 417.º/2 do CPC); haveria ainda que perguntar pela possibilidade de invocar *abuso do direito* correspondente, por *suppressio* (mas também arduamente); isto para não falar do perigo da propositura de acções, possível, fora do prazo de prescrição ou caducidade relativas a direitos disponíveis (cf. o artigo 303.º e 333.º/2 do CC). A permissão de conservação de dados pessoais durante os correspondentes prazos de exercício de direitos permite, melhor do que a regra geral do RGPD, acautelar estas situações.

---

(301) Seja em processo judicial (cf. os artigos 9.º/2 *f)* ou 17.º/3 *e)* do RGPD), em procedimento administrativo junto duma autoridade de controlo (por exemplo contra-ordenacional), perante a administração tributária e aduaneira, etc.

(302) O ponto é relativamente consensual, conforme afirma C. de Terwangne, *Les principes relatifs au traitement* cit., 114 «les données peuvent être conservées à des fins probatoires durant une période correspondant au délai de prescription». Vd. também, por respeito à afectação do tratamento a finalidades ulteriores, Plath, anotação ao artigo 5.º, em *DSGVO BDSG Kommentar,* coord. Kai-Uwe Plath, 3.ª ed., Otto Schmidt, Colónia, 2018, 64-65, (que a p. 65 dá o seguinte exemplo: dados de clientes conservados por comerciante em linha devem ser eliminados, sem prejuízo de deveres legais de arquivo, assim que corrido o prazo de garantia), Roßnagel, anotação ao artigo 5.º, em *Datenschutzrecht* cit., 393-394 (alertando para o esvaziamento da regra pela possibilidade de fins ulteriores, plurais ou variáveis; dá o exemplo dos dados no caso de contrato de transporte), C. de Terwangne, anotação ao artigo 5.º, em *The EU General Data Protection Regulation* cit., 315-317 ou Kotschy, anotação ao artigo 6.º, em *The EU General Data Protection Regulation* cit., 341-343. Diferentemente, o Parecer da CNPD 20/2018 cit., 11v.

(303) Plath, anotação ao artigo 5.º, em *DSGVO BDSG Kommentar* cit., 64-65.

Quanto aos subcontratantes, conforme Parecer da CNPD, «não têm na sua disponibilidade estabelecer prazos de conservação de dados pessoais»; de todo o modo, não significa que não os tratem, de modo que estão também adstritos ao princípio de limitação da conservação (artigo 5.º/1 *e)* do RGPD), ainda que os prazos de conservação com que estão onerados sejam via de regra delimitados pelos do responsável pelo tratamento e inferiores aos deste (cf. o artigo 28.º/3 *g)* do RGPD).

3.3. Tratamento para fins de arquivo de interesse público, investigação científica ou histórica, ou estatísticos

I. A base normativa do artigo 21.º/2 da LE está no artigo 5.º/1 *e)*, 2.ª parte, e no 89.º do RGPD, que o concretiza e é, por sua vez, regulado no artigo 31.º da LE.

Segundo o artigo 5.º/1 *e)*, 2.ª parte, do RGPD: os dados pessoais «podem ser conservados durante períodos mais longos [do que os necessários às finalidades], desde que sejam tratados exclusivamente para fins de arquivo de interesse público[304], ou para fins de investigação científica[305]

---

[304] Não quando de interesse privado (por ex. arquivos de família ou pessoais; arquivos de empresas). Cf. o considerando 158 do RGPD; no direito nacional, o Decreto-Lei n.º 16/93, de 23-jan. Na jurisprudência, TJUE 9-Mar.-2017 *(Salvatore Manni)*, proc. n.º C-398/15 (ECLI:EU:C:2017:197), relativamente à eliminação de informação do registo comercial, com a decisão que se transcreve: «O artigo 6.º, n.º 1, alínea *e)*, o artigo 12.º, alínea *b)*, e o artigo 14.º, primeiro parágrafo, alínea *a)*, da Diretiva 95/46/CE (…), lidos em conjugação com o artigo 3.º da Primeira Diretiva 68/151/CEE do Conselho (…), devem ser interpretados no sentido de que, no atual estado do direito da União, cabe aos Estados-Membros determinar se as pessoas singulares, visadas no artigo 2.º, n.º 1, alíneas *d)* e *j)*, desta última diretiva, podem pedir à autoridade encarregada da manutenção, respetivamente, do registo central, do registo do comércio ou do registo das sociedades que verifique, com base numa apreciação casuística, se se justifica excecionalmente, por razões preponderantes e legítimas relativas à sua situação especial, limitar, findo um prazo suficientemente longo após a dissolução da sociedade em causa, o acesso aos dados pessoais que lhes dizem respeito, inscritos no registo, a terceiros que demonstrem um interesse específico na consulta desses dados». Na doutrina, Herbst, anotação ao artigo 5.º, em *Datenschutz-Grundverordnung Kommentar* cit., 227, Wiese Svanberg, anotação ao artigo 89.º, em *The EU General Data Protection Regulation* cit., 1247, Joaquim de Seabra Lopes, *Publicidade e protecção da privacidade nos registos públicos. Um equilíbrio delicado,* nos *Estudos em homenagem ao Professor Doutor Jorge Ribeiro de Faria,* Coimbra Ed., Coimbra, 2003, 331-358, id., *Publicidade registal e proteção de dados pessoais, Jurismat* 6 (2015), 125-148, ou Catarina Sarmento e Castro, *Privacidade* versus *publicidade: protecção de informações pessoais e actividade registral,* nos *Estudos em Homenagem ao Prof. Doutor Manuel Henrique Mesquita,* Coimbra Ed., Coimbra, 2009, 375-400.

[305] Em sentido lato, abrangendo, por exemplo, o desenvolvimento tecnológico e a «demonstração, a investigação fundamental, a investigação aplicada» e também a financiada pelo sector privado (considerando 159). Vd. também Grages, anotação ao artigo 89.º, em *DSGVO BDSG Kommentar* cit., 708, ou Wiese Svanberg, anotação ao artigo 89.º, em *The EU General Data Protection Regulation* cit., 1249.

ou histórica[306-307] ou para fins estatísticos[308], em conformidade com o artigo 89.º, n.º 1, sujeitos[309] à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados[310-311]» (artigo 5.º/1 *e)*, 2.ª parte; cf. também o artigo 5.º/1 *b)*).

---

[306] Não pode deixar de observar-se, com espanto, a separação, ainda que formal (entenda-se, que não para efeitos de regime), da história e da estatística da investigação científica (vd. também os considerandos 156 a 163, *max.* 157 (onde é feita referência às «ciências sociais»), 159 e 160), o que é muito discutível, para não escrever incorrecto. O legislador euro-comunitário podia, como teve a preocupação de noutros casos fazer (vd. o considerando. 51 sobre o uso do termo «origem racial»), ter exarado um *caveat* a este respeito.

[307] Nos fins históricos está, segundo o considerando 162, também a genealogia, embora seja de notar que o RGPD não vale em relação aos dados de pessoas falecidas (considerando 160; na LE, vd. o artigo 17.º). Vd. também Herbst, anotação ao artigo 5.º, em *Datenschutz-Grundverordnung Kommentar* cit., 227.

[308] Por exemplo, registos de população por áreas, como municípios, áreas metropolitanas, etc. Cf. C. de Terwangne, *Les principes relatifs au traitement* cit., 114.

[309] Aqui seguiu-se (quase) à letra a versão inglesa «subject to» (as outras versões que consultámos optam por diferentes expressões: na alemã «soweit», na francesa «pour autant que», na castelhana «sin perjuicio de», na italiana «fatta salva», na holandesa «mits de»). Sucede que esta é uma expressão idiomática que não pode traduzir-se literalmente. Aliás, tanto assim é que quem esteve encarregado da versão portuguesa se viu forçado a flectir o termo em género e número (o que não sucede no inglês). A questão que ao intérprete de imediato se coloca quando confrontado com a versão portuguesa é: quem está sujeito ou, noutros termos, com que nome concorda «sujeitos»? O adjectivo em causa está no masculino plural, de modo que há que procurar um substantivo do mesmo género e número que o anteceda. Excluído que possa sê-lo o termo «titulares» (dos dados) que surge na primeira parte da al. *e)* do n.º 1 do artigo 5.º, ficam-nos da segunda parte os termos «dados» (pessoais) e «fins» (palavra que aparece três vezes). Ambas as hipóteses são gramaticalmente possíveis (aliás a segunda até mais do que a primeira, porque mais próxima de «sujeitos» e porque mais frequente), mas faz mais sentido que sejam «coisas» – neste caso, dados –, não «fins», sujeitas à aplicação de medidas técnicas e organizativas adequadas. Mas, chegados a este ponto, coloca-se novo problema: dum prisma, é possível dizer que as «coisas», os dados, são sujeitos à «aplicação» de medidas (objecto das medidas), mas doutro não é possível dizer que os dados são os sujeitos (activos) da aplicação das medidas, que só podem ser pessoas. Por isso, deste segundo prisma, na ausência dum sujeito expresso, esperar-se-ia que a oração fosse construída tendo «dados» por sujeito mas o verbo estivesse na voz passiva sem especificação do agente (o dito complemento de agente da passiva; foi esta a via seguida na versão alemã, se bem lemos, sendo da oração sujeito «dados pessoais»: «soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organitorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, (…) verarbeitet werden»). Outras vias passariam por uma oração cujo sujeito fosse «aplicação» (ou «implementação») ou «medidas» e cujo verbo estivesse também na voz passiva (esta foi a via seguida pela versão francesa e pela holandesa: «pour autant que soient mises en oeuvre les mesures techniques et organisationnelles appropriées requises par le present règlement» ou «mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen»). A outra via possível teria sido a seguida na versão italiana («fatta salva») ou na castelhana («sin perjuicio de»).

Não é portanto, nestes casos, necessário provar que a conservação ulterior é necessária a estes fins[312]. Atingidos, no entanto, tais fins, devem ser os dados eliminados ou anonimizados[313]. As medidas técnicas e organizativas em questão asseguram, entre outros[314], o princípio da minimização: um exemplo é a pseudonimização[315] (artigo 89.º/1 do RGPD e 31.º/1 da LE); outro a anonimização (artigo 31.º/1 da LE)[316]. A *ratio* é o reconhecimento da importância e interesse públicos[317] deste tipo de fins e o aproveitamento, via de regra, a todos[318] dos resultados advenientes do tratamento de tais dados subordinado a estes fins; a perda de conhecimento, no caso contrário, seria, de resto, intolerável[319].

---

(310) Como escreve com razão Herbst, anotação ao artigo 5.º, em *Datenschutz-Grundverordnung Kommentar* cit., 230, esta referência às medidas técnicas e organizativas para protecção dos direitos e liberdades dos titulares dos dados é, em comparação com a segunda parte da alínea *b)* do artigo 5.º e em face do artigo 89.º/1, redundante.

(311) É, a nosso ver, discutível se devam, no texto de normas, ser exarados os respectivos fins (neste caso: «a fim de salvaguardar os direitos e liberdades dos titulares dos dados»). Corre-se inclusive o risco de, por interpretação, chegar-se a conclusão diversa ou não inteiramente coincidente (ainda que aqui não seja este necessariamente o caso). Corre-se igualmente o risco de duplicações (como é o caso, bastando para o efeito confrontar-se o disposto no artigo 89.º/1 do RGPD) ou assintonias (cf. o artigo 5.º/1 *b)*). No RGPD, contudo, vários são os exemplos em que redacções deste género foram adoptadas.

(312) Assim, Herbst, anotação ao artigo 5.º do RGPD, em *Datenschutz-Grundverordnung Kommentar* cit., 230 (falando, a este respeito, de um privilégio dos referidos fins). Contra, Roßnagel, anotação ao artigo 5.º, em *Datenschutzrecht* cit., 393.

(313) Roßnagel, anotação ao artigo 5.º, em *Datenschutzrecht* cit., 393.

(314) Daí o «nomeadamente» no artigo 89.º/1.

(315) Cf., por ex., TJUE 16-dez.-2008 (*Heinz Huber v. Bundesrepublik Deutschland*), proc. n.º C-524/06 (ECLI:EU:C:2008:724), § 65.

(316) Estas medidas – típicas em determinados sectores, como a pesquisa médica – podem não ser as mais adequadas no caso concreto, como chama, com razão, a atenção Wiese Svanberg, anotação ao artigo 89.º, em *The EU General Data Protection Regulation* cit., 1247, com o seguinte exemplo: em matéria de dados preservados para fins de arquivo pode fazer pouco sentido a anonimização ou pseudonimização, «uma vez que a remoção do nexo entre as pessoas e os eventos negaria o propósito do tratamento»; como enfatiza o artigo 89.º/1 («Sempre que esses fins possam ser atingidos por novos tratamentos (…)»), tais medidas só devem ser usadas quando não desvirtuarem o propósito do tratamento.

(317) Ainda que de financiamento privado, como o pode ser a investigação científica.

(318) Vd. também Herbst, anotação ao artigo 5.º, em *Datenschutz-Grundverordnung Kommentar* cit., 227 e 231, ou Wiese Svanberg, anotação ao artigo 89.º, em *The EU General Data Protection Regulation* cit., 1242-1243.

(319) Cf. também o considerando 157. Por isso, pode dizer-se, com Wiese Svanberg, anotação ao artigo 89.º, em *The EU General Data Protection Regulation* cit., 1243, que, neste caso, não é questão de saber se podem os dados ser tratados, mas que salvaguardas devam ser impostas e associadas no momento em que o sejam.

II. Questiona-se se exista, no artigo 5.º/1 *e)*, 2.ª parte, uma excepção à regra de que os dados devem ser tratados unicamente durante o período necessário à prossecução dos fins do tratamento.

Na segunda parte da alínea *e)* do n.º 1 do artigo 5.º do RGPD é dito que os dados podem ser conservados «durante períodos mais longos». À letra, o dizer-se que os prazos podem ser «mais longos» pressupõe um referente em função do qual se afere a comparação, ou seja, um referente cuja característica seja os prazos serem menos longos. Este consta da primeira parte da alínea *e)*: os dados pessoais são «conservados (...) apenas durante o período necessário para as finalidades para as quais são tratados». Isto significa que, quando se escreveu «durante períodos mais longos», se pressupôs como termo de comparação «o período necessário para as finalidades para as quais [os dados] são tratados», o mesmo é dizer que, nos casos previstos na segunda parte, «os dados pessoais podem ser conservados durante períodos mais longos» do que «o período necessário para as finalidades para as quais são tratados». Esta redacção, portanto, inculca a ideia de que o tratamento de dados para os fins referidos na segunda parte pode fazer-se por períodos durante os quais não seja já necessário o tratamento.

Não nos parece, todavia, ser este o melhor entendimento. Deixando de ser o tratamento *necessário* aos fins de arquivo público, de investigação científica ou histórica e estatísticos, também o seu tratamento – aqui incluída a sua conservação (artigo 4.º/2 do RGPD) –, deve cessar. A própria referência a *«períodos mais longos»*, em detrimento doutras possíveis redacções, significa não se ter querido perpetuar o tratamento subordinado às mencionadas finalidades: permitem-se períodos mais longos, mas não perpétuos. O problema aqui é que, do prisma da *limitação da conservação,* tais *finalidades* são, por *natureza, duradouras:* os fins de investigação científica, aqui obviamente inclusa a histórica, são, no actual estádio civilizacional, *temporalmente indeterminados;* os fins de arquivo de interesse público e os estatísticos mantêm-se durante períodos muito alargados e, no caso dos de arquivo público, potestativamente dependentes dum acto de autoridade. A duração duns e

doutros não é a *priori* determinável. Por outro lado, *do prisma da limitação das finalidades,* elas são muito difíceis de circunscrever, quando não mesmo também indetermináveis.

Chegados a este ponto, existem duas hipóteses interpretativas: «prazos mais longos» do que «o período necessário para as finalidades para as quais são [primariamente] tratados»[320] ou «prazos mais longos» em geral, ou seja, «mais longos» do que o que ocorreria na maioria dos casos[321]. Preferimos a conjugação das duas hipóteses, que não se excluem, e respondemos de forma negativa à questão inicialmente formulada, ou seja, em rigor, não pode, neste caso, de excepção falar-se.

III. O enquadramento do artigo 21.º/1 da LE é, pois, dado pelo artigo 5.º/1 *e)* do RGPD, a que aquele pouco acrescenta, além de aspectos circunstanciais, alguns deles duvidosos.

O artigo 21.º/1 fala de tratamentos em relação aos quais, «pela natureza e finalidade», «não seja possível determinar antecipadamente o momento em que o mesmo deixa[rá] de ser necessário», de que os fins de arquivo de interesse público, de investigação científica ou histórica, ou estatísticos seriam exemplo. O RGPD, na verdade, não concede este «privilégio» a outros fins que não estes, de modo que não pode ser o elenco exemplificativamente interpretado. O RGPD não se refere também a «natureza», de maneira que há que sinonimizá-la a «finalidade», como um acrescento de prolixidade. A referência a impossibilidade de determinação antecipada do momento em que o tratamento deixe de ser necessário deve entender-se como descritiva dos fins em apreço, mas não constitutiva duma categoria à parte.

---

[320] Cf., em linha com este entendimento, o considerando 156: «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 (...)». É esta também a interpretação de Roßnagel, anotação ao artigo 5.º, em *Datenschutzrecht* cit., 393, que entende que as finalidades em relação às quais se afere a «maior longueza» são as primárias, explicando que a excepção ao princípio da limitação da conservação tem como consequência que, para os referidos fins (secundários), podem ser os dados conservados durante mais tempo do que seja necessário para atingir o fim originário (primário).

[321] Esta interpretação tem em seu favor acolher em si a hipótese de o tratamento ter sido primariamente feito tendo em vista tais fins.

3.4. Direito ao apagamento

O artigo 21.º/4 da LE impede o exercício do direito ao apagamento enquanto corra «um prazo de conservação de dados imposto por lei».

Tendo em conta a distinção a que se procede no n.º 1 entre norma legal e regulamentar, «lei» parece corresponder no n.º 3 apenas às normas legais do n.º 1.

O artigo 17.º/3 do RGPD tolhe, com efeito, o *ius delendi* na hipótese de cumprimento de dever legal que exija o tratamento, com que se harmoniza e deve ser em conformidade interpretado o n.º 4 do artigo 21.º da LE[322].

3.5. Dados relativos a declarações contributivas para efeito de aposentação ou reforma

O propósito no n.º 8 do artigo 21.º é o de «auxiliar o titular na reconstituição das carreiras contributivas», exercício nem sempre fácil, sobretudo quando estejam em causa rendimentos que remontem a épocas mais recuadas sem informação disponível em formato electrónico.

Não é exacto o que seja o tratamento «sem limite de prazo»: cessando a finalidade, de resto na própria norma exarada, cessa o fim do tratamento e, nessa medida, devem ser os dados pessoais eliminados[323] (artigo 21.º/4).

O acrescento «desde que sejam adotadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados» era desnecessária (cf. já o artigo 5.º/1 *e)* e 89.º/1 do RGPD).

É questionável se, na situação em apreço, estejam ainda em causa fins de arquivo de interesse público, posto que tendamos a uma resposta afirmativa.

---

[322] Diversamente, Parecer da CNPD 20/2018, 11v.-12.

[323] Se a cessação dos fins ocorrer, todavia, com a morte do titular dos dados, o problema assume contornos diversos, visto que o RGPD não se aplica aos dados pessoais de pessoas falecidas. Vd., porém, o artigo 17.º e sobre as perplexidades por este suscitadas Luís Poças, *O tratamento de dados de pessoas seguras falecidas,* RDES LX (2019) 1/4, 237-279.

4. Conclusão

Consensual na teoria, fonte de inúmeras controvérsias na prática, o tema dos prazos de conservação de dados pessoais está longe de se encontrar esgotado. O RGPD não densifica a matéria, nem se preocupa, talvez deliberadamente (e bem), em torná-la mais facilmente «operacional». Novos diplomas procuraram fazê-lo, a começar pela LE no artigo 21.º ou a Lei n.º 59/2019 no artigo 12.º, em termos cuja compatibilização com o RGPD tem sido discutida, mas ainda assim com uma «margem» que permite preservar parte da original flexibilidade do diploma base. Outros diplomas, como o Regulamento aprovado pela Portaria n.º 112/2023, mesmo não tendo por objecto apenas dados pessoais, levaram ainda mais longe o intento, petrificando, questionavelmente, um regime que não pode deixar de ser flexível. Vejamos, pois, o que o futuro nos trará.

* Professor Associado da Universidade Europeia. Professor Associado Convidado da Universidade Lusíada – Angola e no Instituto Superior de Psicologia Aplicada (ISPA). Doutor em Direito pela Faculdade de Direito de Lisboa. Investigador do IDPCC e do CIJIC. Jurisconsulto. Conferencista. Exerceu as funções de Juiz de Direito entre setembro de 2005 e janeiro de 2022, estando atualmente em situação de licença sem retribuição.

Este artigo foi entregue para publicação no dia 13 de novembro de 2023.

9 | O DAY AFTER DO ACÓRDÃO DO TRIBUNAL CONSTITUCIONAL N.º 268/2022

*Duarte Rodrigues Nunes**

1. Introdução

No transato ano de 2022, pouco tempo após a prolação do Acórdão do TC n.º 268/2022, escrevemos um artigo em que formulámos fortes críticas a este aresto[324]. Na sequência desse artigo, fomos convidados para proferir algumas palestras sobre o tema, uma das quais no Centro de Estudos Judiciários, no âmbito da formação contínua de Magistrados. Subsequentemente, fomos ouvidos pelo Grupo de Trabalho dos Metadados da 1.ª Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República, no âmbito do procedimento legislativo tendente à reformulação da Lei n.º 32/2008, de 17 de julho, após a prolação do Acórdão do TC n.º 268/2022, tendo então elaborado um pequeno estudo, que é o ponto de partida para o presente artigo.

2. O Acórdão *Digital Rights* do Tribunal de Justiça da União Europeia e o Acórdão do Tribunal Constitucional n.º 268/2022

No rescaldo dos terroristas de Madrid (11 de março de 2004) e de Londres (7 de julho de 2005), em que foi a reconstituição das comunicações eletrónicas entre os vários intervenientes das redes terroristas em causa que permitiu às autoridades perceberem as relações existentes entre eles, o Parlamento Europeu e o Conselho adotaram a Diretiva 2006/24/CE, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

A Diretiva 2006/24/CE, que visou harmonizar as disposições dos Estados-Membros relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de

(324) DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, pp. 9-58.

comunicações em matéria de conservação de dados de tráfego, dados de localização relativos pessoas singulares e/ou a pessoas coletivas e dados conexos necessários para identificar o assinante ou o utilizador registado por eles gerados ou tratados (correntemente designados como metadados[325]) para fins de investigação, deteção e repressão de crimes graves, tal como definidos no Direito nacional de cada Estado-Membro, obrigou os Estados-Membros a tomarem medidas para garantir a conservação dos dados necessários para:

a) encontrar e identificar a fonte e/ou o destino de uma comunicação;

b) identificar a data, a hora e a duração de uma comunicação;

c) identificar o tipo de comunicação;

d) identificar o equipamento de telecomunicações dos utilizadores ou o que se considera ser o seu equipamento; e

e) identificar a localização do equipamento de comunicação móvel (incluindo no caso de chamadas telefónicas falhadas), quando gerados ou tratados e armazenados (no caso de dados telefónicos) ou registados (no caso de dados da *Internet*) por fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações que estejam sob a jurisdição do Estado-Membro em questão, no contexto da oferta de serviços de comunicação.

Tal Diretiva excluía expressamente do seu âmbito de aplicação a conservação de dados de conteúdo de comunicações (*cfr*. arts. 1.º, n.º 2, e 5.º, n.º 2).

A Diretiva 2006/24/CE foi transposta para o Direito português através da Lei n.º 32/2008.

Todavia, a Diretiva 2006/24/CE foi declarada inválida pelo TJUE, no âmbito de um reenvio prejudicial ao abrigo do art. 267.º do TFUE, através do seu Acórdão 8 de abril de 2014, *Digital Rights* Ireland Ltd e Kärntner Landesregierung[326].

---

[325] Sem prejuízo do escasso rigor dessa designação.

[326] Usualmente designado Acórdão Digital Rights.

Nesse aresto, o TJUE entendeu que a conservação dos dados referidos na Diretiva e o acesso das autoridades a esses dados restringem, de forma intensa (embora sem afetar o seu conteúdo essencial), os direitos tutelados pelos arts. 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE), sendo que, nos termos do artigo 52.º, n.º 1, da Carta, qualquer restrição ao exercício dos direitos e liberdades garantidos

pela CDFUE deve estar prevista na lei e respeitar o conteúdo essencial desses direitos e liberdades e, por força dos ditames do princípio da proporcionalidade, só podem ser introduzidas restrições a esses direitos e liberdades se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros.

E, nessa conformidade, o TJUE considerou que, apesar de não ocorrer qualquer restrição do conteúdo essencial dos referidos direitos fundamentais e de estar em causa a prossecução de fins legítimos (a resposta à criminalidade grave e, em última análise, a salvaguarda da segurança pública), a Diretiva 2006/24/CE restringia, de forma desproporcionada, os mencionados direitos fundamentais, uma vez que:

a) abrangia, de uma forma indiscriminada, todas as pessoas que utilizassem serviços de comunicações eletrónicas, inclusivamente pessoas em relação às quais não existiam indícios de que o seu comportamento pudesse ter um nexo, ainda que indireto ou longínquo, com infrações graves e sem prever qualquer exceção quanto a comunicações abrangidas pela proteção do segredo profissional;

b) não exigia nenhuma relação entre os dados conservados e uma ameaça para a segurança pública nem limitava a conservação a dados relativos a um período de tempo, a uma zona geográfica determinada e/ou a um círculo de pessoas determinadas que possam estar implicadas, de alguma forma, numa infração grave

nem a dados relativos a pessoas cuja conservação pudesse contribuir para a prevenção, a deteção ou a repressão de infrações graves;

c) não estabelecia critérios objetivos que permitissem delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior à prevenção, deteção ou punição de infrações graves;

d) não limitava o acesso e a utilização posterior dos dados conservados à prevenção e à deteção de crimes graves nem estabelecia critérios objetivos que permitam limitar o número de pessoas com autorização de acesso e de utilização posterior dos dados conservados ao estritamente necessário tendo em conta o objetivo prosseguido;

e) não exigia que o acesso aos dados conservados dependesse de um pedido fundamentado no âmbito de procedimentos de prevenção ou de deteção de crimes ou de uma ação penal e fosse objeto de controlo prévio por um órgão jurisdicional ou entidade administrativa independente e também não obrigava os Estados-Membros a preverem esses requisitos no seu Direito interno; f) no que respeita à duração da conservação dos dados, que impunha que fosse fixada entre 6 e 24 meses, não procedia a qualquer distinção entre as categorias de dados em função da sua eventual utilidade relativamente ao objetivo prosseguido ou em função das pessoas em causa nem impunha que a determinação do período de conservação deveria basear-se em critérios objetivos, a fim de garantir que se limitava ao estritamente necessário; e

f) quanto à segurança e à proteção dos dados conservados pelos fornecedores de serviços de comunicações eletrónicas, (1) não obrigava os Estados-Membros a estabelecerem regras específicas e adaptadas à grande quantidade de dados cuja conservação era imposta, ao caráter sensível desses dados e ao risco de acesso ilícito aos mesmos, (2) não garantia a aplicação, pelos referidos fornecedores, de um nível particularmente elevado de proteção,

(3) não impunha a destruição definitiva dos dados no termo do período de conservação dos mesmos e (4) não impunha a obrigação de os metadados serem conservados no território da União Europeia (pelo que não se poderia considerar que estivesse plenamente garantida a fiscalização do respeito das exigências de proteção e de segurança por uma entidade independente, tal exigido pelo art. 8.°, n.º 3, da CDFUE).

Na sequência deste acórdão do TJUE, passou a discutir-se se a Lei n.º 32/2008 era, ou não, incompatível com o Direito da União Europeia e se, consequentemente, a conservação de dados à luz dessa Lei era, ou não, admissível à luz da e da CDFUE[327].

Contudo, a principal consequência, entre nós, do Acórdão *Digital Rights*, foi o Acórdão do TC n.º 268/2022.

Assim, por via do aludido aresto, o TC, embora com um voto de vencido, declarou inconstitucionais, com força obrigatória geral:

a) a norma constante do art. 4.º da Lei n.º 32/2008, conjugada com o art. 6.º da mesma Lei, por violação do disposto nos arts. 35.º, n.ºs 1 e 4, e 26.º, n.º 1, em conjugação com o art. 18.º, n.º 2, todos da CRP; e

b) a norma constante do art. 9.º da Lei n.º 32/2008 (na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros), por violação do disposto nos arts. 35.º, n.º 1, e 20.º, n.º 1, em conjugação com o art. 18.º, n.º 2, todos da CRP[328].

---

[327] *Vide* a este respeito, com maiores desenvolvimentos, DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, pp. 22-23.

[328] Note-se, porém, que o TC (tal como o TJUE, embora relativamente à CDFUE), em momento algum considerou inconstitucional a utilização probatória de metadados nem a obtenção de metadados em tempo real (no mesmo sentido, RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", in *RMP*, n.º 172, pp. 35 e ss.).

O Acórdão n.º 268/2022 foi prolatado no âmbito de um pedido de declaração de inconstitucionalidade dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008, em sede de fiscalização abstrata sucessiva à luz do art. 281.º da CRP, formulado pela Provedora da Justiça.

Esta declaração da inconstitucionalidade veio suscitar a questão da admissibilidade, ou não, da obtenção e valoração, nos processos em curso, de metadados que tenham sido conservados pelos respetivos operadores e das provas obtidas através desses metadados. E, ainda mais grave, veio abrir a possibilidade de, se forem interpostos recursos de revisão ao abrigo do art. 449.º, n.º 1, als. e) e f), do CPP que sejam julgados procedentes, serem revertidas condenações transitadas em julgado em processos nos quais, em observância de todas as garantias e esgotados todos os mecanismos de recurso de que os arguidos tenham decidido lançar mão, se provou, para além da dúvida razoável, o cometimento do crime ou dos crimes pelos quais foram condenados[329].

3. A jurisprudência do Tribunal de Justiça da União Europeia posterior ao Acórdão *Digital Rights*

Após ter anulado a Diretiva 2006/24/CE, o TJUE passou a apreciar a questão da conservação de metadados para efeitos de investigação criminal com base no art. 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, interpretado à luz dos arts. 7.º, 8.º e 52.º, n.º 1, da CDFUE.

[329] No entanto, tais recursos têm sido julgados improcedentes pelo STJ (cfr., entre outros, Acórdãos do STJ de 21/09/2022, 10/11/2022, 19/01/2023, 01/02/2023, 11/05/2023, 21/06/2023 e 29/06/2023), com fundamento no disposto no art. 282.º, n.º 3, 2.ª parte, da CRP, porquanto o TC, no Acórdão n.º 268/2022 não afastou a ressalva dos casos julgados, entendimento cuja bondade não cumpre analisar no âmbito do presente artigo, atento o respetivo objeto.

Assim, no Acórdão Tele2 Sverige AB e Secretary of State for the Home Department, o TJUE entendeu que:

a) A CDFUE proíbe a conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica;

b) A CDFUE impõe que os dados sejam conservados no território da União Europeia; e

c) A CDFUE apenas permite o acesso aos dados conservados para efeitos de luta contra a criminalidade grave e desde que esse acesso esteja sujeito a controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente.

No Acórdão Ministerio Fiscal, o TJUE entendeu que a CDFUE permite o acesso das autoridades públicas a dados de base como o apelido, o nome próprio, a morada dos titulares dos cartões SIM ativados num telemóvel roubado, para efeitos de luta contra a criminalidade grave.

No Acórdão Privacy International, o TJUE considerou que a CDFUE proíbe a imposição, aos prestadores de serviços de comunicações eletrónicas, para efeitos da salvaguarda da segurança nacional, da transmissão generalizada e indiferenciada de dados de tráfego e de dados de localização aos serviços de segurança e de informações.

No Acórdão *La Quadrature du Net,* o TJUE entendeu que a CDFUE proíbe a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização a título preventivo, mas permite:

a) A conservação generalizada e indiferenciada de dados de tráfego e de dados de localização para salvaguarda da segurança nacional, quando o Estado-Membro em causa enfrente uma ameaça grave e que seja real e atual ou previsível, desde que a decisão que prevê tal imposição possa ser objeto de fiscalização efetiva (por um órgão jurisdicional ou por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos) e essa

conservação apenas ocorra durante um período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça;

b) A conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, desde que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado; e

c) A conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública.

No Acórdão Prokuratuur, o TJUE considerou que:

a) A CDFUE proíbe o acesso de autoridades públicas a dados de tráfego ou de localização para fins de prevenção, investigação, deteção e perseguição de infrações penais, sem que esse acesso esteja circunscrito a processos que visem a luta contra a criminalidade grave ou a prevenção de ameaças graves à segurança pública, independentemente da duração do período em relação ao qual o acesso aos referidos dados é solicitado e da quantidade ou da natureza dos dados disponíveis sobre tal período; e

b) A atribuição da competência ao MP para autorizar o acesso aos dados de tráfego e aos dados de localização para fins de investigação criminal viola a CDFUE, pois a missão do MP é dirigir a investigação e exercer a ação penal.

No Acórdão G. D. e Commissioner of An Garda Síochána, o TJUE entendeu que a CDFUE proíbe a conservação generalizada e indiferenciada de dados

de tráfego e de dados de localização a título preventivo para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, mas permite:

a) A conservação seletiva de dados de tráfego e de dados de localização, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional, delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;

b) A conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional, por um período temporalmente limitado ao estritamente necessário; e

c) A conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional, desde que (1) esteja assegurado, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e (2) as pessoas visadas disponham de garantias efetivas contra eventuais abusos.

Finalmente[330], no Acórdão *SpaceNet* e *Telekom Deutschland,* o TJUE considerou que a CDFUE proíbe a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização a título preventivo para

[330] Posteriormente a este aresto, o TJUE proferiu o Acórdão A. G. e Lietuvos Respublikos generalinė prokuratūra, em que, apesar de versar sobre a utilização de metadados conservados, o Tribunal analisa uma questão diversa, mais concretamente, a de saber se é admissível, à luz da CDFUE, a utilização, em investigações relativas a ilícitos disciplinares relativos a atos de corrupção, de metadados que haviam sido conservados pelos prestadores de serviços de comunicações eletrónicas. O TJUE considerou que tal não é admissível, por violação dos arts 7.º, 8.º e 52.º, n.º 1, da CDFUE, uma vez que não estava em causa o afastamento de qualquer ameaça à segurança interna ou à segurança pública nem a luta contra a criminalidade grave.

Efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, mas permite

a) A conservação generalizada e indiferenciada de dados de tráfego e de dados de localização para salvaguarda da segurança nacional, quando o Estado-Membro em causa enfrente uma ameaça grave e que seja real e atual ou previsível, desde que a decisão que prevê tal imposição possa ser objeto de fiscalização efetiva (por um órgão jurisdicional ou por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos) e essa conservação apenas ocorra durante um período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça;

b) A conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, desde que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;

c) A conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional, por um período temporalmente limitado ao estritamente necessário; e

d) A conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública, desde que (1) esteja assegurado, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e (2) as pessoas visadas disponham de garantias efetivas contra eventuais abusos.

Em suma, de acordo com a jurisprudência do TJUE, em matéria de conservação de metadados, a CDFUE impõe que os dados sejam conservados no território da União Europeia e proíbe a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, a título preventivo, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, mas permite:

1. A conservação generalizada e indiferenciada de dados de tráfego e de dados de localização para salvaguarda da segurança nacional, quando o Estado-Membro em causa enfrente uma ameaça grave, real e atual ou previsível, desde que essa conservação apenas ocorra durante um período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça, contanto que a decisão que determina a conservação seja efetivamente fiscalizada por um órgão jurisdicional ou por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos;

2. A conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, desde que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;

3. A conservação generalizada e indiferenciada, por um período temporalmente limitado ao estritamente necessário, dos endereços IP atribuídos à fonte de uma ligação, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional; e

4. A conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública.

E, relativamente ao acesso aos metadados conservados, a CDFUE apenas permite o acesso aos dados conservados para efeitos de luta contra a criminalidade grave e desde que esse acesso esteja sujeito a controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente (que não inclui o MP, pois é o titular da ação penal).

4. A jurisprudência dos Tribunais Judiciais portugueses na sequência do Acórdão do Tribunal Constitucional n.º 268/2022 em matéria de obtenção e/ou valoração de metadados conservados

No seguimento do Acórdão do TC n.º 268/2022, surgiram, na jurisprudência dos Tribunais comuns, dois entendimentos em matéria de obtenção e/ou valoração de metadados conservados.

Assim, para um primeiro entendimento[331], por força da declaração de inconstitucionalidade com força obrigatória geral dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008, não é admissível obter e a valorar, em processos penais, metadados conservados à luz da Lei n.º 41/2004, de 18 de agosto, pelos prestadores de serviços de comunicações eletrónicas e obtidos à luz do art. 189.º, n.º 2, do CPP ou da Lei n.º 109/2009, de 15 de setembro, argumentando-se que:

a) Dado que a Lei n.º 41/2004 é relativa à proteção contratual no contexto das relações estabelecidas entre as empresas fornecedoras de serviços de comunicações eletrónicas e os seus clientes, não é lícito recorrer a este diploma para efeitos de investigação criminal[332];

b) Aplicar o regime dos arts. 187.º a 189.º do CPP, da Lei n.º 41/2004 e da Lei n.º 109/2009, significaria *"deixar entrar pela janela"* aquilo a que o Acórdão do TC n.º 268/2022 "fechou a porta", pois o regime que resultaria da aplicação dos arts. 187.º a 189.º do CPP, da Lei n.º 41/2004 e da Lei n.º 109/2009 padece da mesma falta de garantias, no plano da investigação criminal, que levou à declaração de inconstitucionalidade dos arts. 4.º, 6.º e 9.º da Lei nº 32/2008[333];

---

[331] Acolhido nos Acórdãos da RL de 25/10/2022, da RP de 07/09/2022, 07/12/2022 e 24/05/2023, da RC de 12/10/2022 e da RE de 25/10/2022, 28/02/2023, 09/05/2023 e 12/09/2023.

[332] Cfr. Acórdãos da RP de 07/12/2022 e da RC de 12/10/2022.

[333] Cfr. Acórdão da RP de 07/12/2022.

c) Aplicar a Lei n.º 109/2009 implicaria defraudar o espírito do legislador, pois o desaparecimento da norma especial (*in casu,* os arts. 3.º e 9.º da Lei n.º 32/2008) não legitima a aplicação da norma geral (*in casu,* as normas da Lei n.º 109/2009)[334];

d) Os Tribunais não podem substituir-se ao legislador, suprindo omissões de onde resultam graves inconvenientes para a investigação criminal[335];

e) Dado que não existe qualquer identidade formal ou material entre o catálogo de crimes do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 e o catálogo de crimes dos arts. 187.º, n.º 1, e 189.º do CPP, não há revogação do segundo pelo primeiro dos dois regimes e, por isso, não se tem de aplicar, por repristinação, nenhuma norma do CPP (o que, de resto, implicaria o desrespeito pela opção do legislador de ter criado um catálogo mais restrito no art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 em vez de considerar como "crimes graves" os crimes constantes do catálogo do n.º 1 do art. 187.º do CPP)[336];

f) "Caindo" a Lei n.º 32/2008 e na impossibilidade de aplicação do CPP e da Lei n.º 41/2004, recorrer às normas da Lei n.º 109/2009 seria seguir um caminho espúrio, tendo em conta a declaração de inconstitucionalidade e os fundamentos que a determinaram, não sendo lícito recorrer a "atalhos" como a invocação do disposto no art. 189.º do CPP ou na Lei n.º 109/2009 (para mais quando o art. 11.º, n.º 2, desta Lei determina que o disposto nos arts. 12.º a 19.º dessa Lei não prejudica o regime da Lei n.º 32/2008)[337];

g) Tendo em conta os fundamentos da declaração de invalidade da Diretiva 2006/24/CE pelo TJUE, o regime da Lei n.º 32/2008 teria de ser ainda mais restritivo (e daí a declaração de inconstitucionalidade dos arts. 4.º, 6.º e 9.º desta Lei), sendo certo que o regime do art. 189.º, n.º 2, do CPP é menos exigente do que o regime da Lei n.º 32/2008[338]; e

---

[334] Cfr. Acórdãos da RP de 07/12/2022 e da RC de 12/10/2022.

[335] Cfr. Acórdãos da RP de 07/12/2022 e da RC de 12/10/2022.

[336] Cfr. Acórdão da RC de 12/10/2022.

[337] Cfr. Acórdão da RC de 12/10/2022.

[338] CCfr. Acórdão da RC de 12/10/2022.

h) Obter ou valorar metadados conservados com base no art. 189.º, n.º 2, do CPP, na Lei n.º 41/2004 e na Lei n.º 109/2009 levaria a que a declaração de inconstitucionalidade produzisse o efeito contrário àquele que pretendeu (pois permitiria a aplicação de um regime menos restritivo do que o regime dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008)[339].

Diversamente, para um segundo entendimento[340], apesar da declaração de inconstitucionalidade com força obrigatória geral dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008, a obtenção e a valoração, em processos penais, de metadados conservados à luz da Lei n.º 41/2004, de 18 de agosto, pelos prestadores de serviços de comunicações eletrónicas, para fins de faturação dos serviços prestados continua a ser admissível[341], porquanto essas normas não foram declaradas inconstitucionais pelo TC.

5. A jurisprudência do Tribunal Europeu dos Direitos Humanos

No Acórdão *Big Brother Watch* e Outros c. Reino Unido, em que estava em causa a apreciação da compatibilidade da interceção massiva (e, como tal, generalizada e indiferenciada) de dados de conteúdo de comunicações (sob a forma de dados informáticos) e de dados de tráfego *(bulk interception)*[342] com o art. 8.º da CEDH, o TEDH, pese embora tenha condenado o Reino Unido, considerou que:

a) A interceção massiva (e, como tal, generalizada e indiferenciada) de dados de conteúdo de comunicações (sob a forma de dados informáticos) e de dados de tráfego *(bulk interception)*, por si só, não viola o art. 8.º da CEDH, contanto que sejam observadas determinadas garantias mínimas;

---

[339] Cfr. Acórdão da RC de 12/10/2022.

[340] Acolhido nos Acórdãos do STJ de 21/06/2023, da RL de 26/01/2023 e 22/02/2023, da RP de 29/03/2023, da RC de 21/06/2023 e 27/09/2023, da RE de 28/06/2023 e da RG de 02/05/2023.

[341] Nos termos previstos no art. 189.º, n.º 2, do CPP e na Lei n.º 109/2009, de 15 de setembro.

[342] Esta interceção massiva de dados de conteúdo e de dados de tráfego consiste em intercetar e recolher, de forma massiva, nos cabos óticos utilizados para a realização de comunicações, os dados relativos a todas as comunicações eletrónicas (incluindo os dados de conteúdo) realizadas por todos os dispositivos

b) No caso da vigilância generalizada e indiferenciada (e que, por isso, não tem alvos determinados e delimitados), como é o caso da interceção massiva de dados de conteúdo e de dados de tráfego, as salvaguardas são ainda mais essenciais do que no caso da vigilância seletiva dirigida a pessoas determinadas (*targeted interception*);

c) Na medida em que a interceção massiva de dados de conteúdo e de dados de tráfego, pela sua própria natureza, é, por um lado, preventiva e prévia à existência de qualquer *notitia criminis* ou ao conhecimento da existência de uma ameaça concreta à segurança nacional e, por outro lado, generalizada e indiferenciada, não é possível aplicar-lhe duas das seis salvaguardas mínimas exigidas pelo TEDH no seu *case law* relativo às medidas de vigilância seletivas (*v.g.*, as escutas telefónicas): delimitação, pelo legislador, de um catálogo de crimes e de alvos e existência de uma suspeita fundada da prática de um crime do catálogo;

d) No entanto, ainda assim terão de ser existir salvaguardas mínimas no Direito interno dos Estados para que a interceção massiva de dados

---

conectados a uma determinada rede de comunicações. A interceção massiva de dados de conteúdo de comunicações (sob a forma de dados informáticos) e de dados de tráfego passa por 4 fases:

1. Interceção e conservação dos dados informáticos relativos ao conteúdo de comunicações eletrónicas (dados de conteúdo) e dos dados relativos a comunicações (dados de tráfego);

2. Tratamento e seleção, de forma automatizada e com utilização de critérios de seleção, dos dados de conteúdo e de tráfego previamente conservados;

3. Exame, por analistas, dos dados de conteúdo e de tráfego previamente selecionados; e

4. Conservação dos dados considerados relevantes após o respetivo exame e utilização desses dados, incluindo no que tange à sua partilha com outras entidades (nacionais ou estrangeiras).

No caso decidido pelo TEDH no citado aresto, as autoridades inglesas procediam à recolha, de forma massiva, para fins de segurança nacional, de todos os dados de conteúdo e dados de tráfego de todas as comunicações realizadas; subsequentemente, os dados obtidos eram sujeitos a um processo de seleção automatizado, com utilização de inteligência artificial, baseado em critérios abstratos de seleção, sendo destruídos os dados que não fossem considerados passíveis de possuírem relevância; seguidamente, os dados considerados como passíveis de possuírem relevância eram alvo de um segundo processo de seleção, agora manual, levada a cabo por analistas, sendo destruídos os dados que fossem considerados irrelevantes; e, por fim, os dados que haviam considerados pelos analistas como podendo possuir relevância eram alvo de conservação para ulterior utilização, sendo destruídos automaticamente ao fim de alguns meses.

de conteúdo e de dados de tráfego observe as exigências do art. 8.º da CEDH, mais concretamente:

- O Direito interno deverá prever, de forma clara, as circunstâncias em que as autoridades poderão lançar mão da interceção massiva de dados de conteúdo e de dados de tráfego, a duração da execução da medida, o procedimento relativo ao exame, utilização e conservação dos dados recolhidos, as precauções a observar relativamente à transmissão dos dados a outras entidades e em que circunstâncias os dados deverão ser apagados ou destruídos;
- Em face do carácter necessariamente secreto da interceção massiva de dados de conteúdo e de dados de tráfego (sob pena de inutilidade), a supervisão e o controlo efetivos (por uma entidade independente do poder executivo, que não é forçoso que seja um Juiz) da implementação da medida em todas as fases suprarreferidas (e não apenas relativamente à autorização do recurso à medida e à sua renovação) é absolutamente essencial para evitar abusos, incluindo no que tange à necessidade e à proporcionalidade do recurso à interceção em massa no caso concreto;
- O Direito interno deverá prever mecanismos que permitam às pessoas que suspeitem de que os seus dados foram alvo de interceção em massa contestar, de forma efetiva e não meramente aparente, a legalidade da medida e/ou a compatibilidade do regime da interceção em massa com a CEDH, sem dependência de qualquer notificação de que os seus dados foram alvo da medida; para tal, a entidade competente para apreciar a impugnação deverá ser independente do poder executivo (mas não tendo de ser necessariamente um Tribunal) e o procedimento terá de ser equitativo, devendo incluir a possibilidade de contraditório (na medida do possível) e a fundamentação da decisão, que deverá ser juridicamente vinculativa para o poder executivo, ao ponto de poder determinar a cessação de uma interceção ilegal e a destruição dos dados obtidos ou conservados de forma ilegal.

O TEDH também tem entendido que a proteção dos direitos fundamentais inclui o dever de as autoridades levarem a cabo uma investigação efetiva e eficaz (no sentido de serem utilizados meios de investigação que se mostrem necessários para investigar no caso concreto) em ordem a investigar os crimes que atinjam algum dos direitos fundamentais garantidos pela CEDH, desde logo, no caso de homicídios, tendo em conta o disposto no art. 2.º da CEDH[343].

No que concerne à obtenção de metadados em investigações criminais, o TEDH considera que a não obtenção de metadados cuja obtenção se mostre necessária para uma determinada investigação criminal de crimes cometidos através da Internet ou com utilização da Internet é incompatível com o art. 8.º da CEDH (que também inclui um dever positivo de as autoridades levarem a cabo uma investigação efetiva e eficaz relativamente a crimes que lesem os direitos fundamentais tutelados por esse preceito da CEDH) se essa não obtenção puser em causa a eficácia dessa mesma investigação[344].

De resto, no Acórdão K.U. c. Finlândia é particularmente evidente a censura do TEDH à excessiva importância que foi atribuída pelas autoridades finlandesas à confidencialidade dos dados de tráfego dos internautas na investigação de uma situação em que um determinado indivíduo publicou um anúncio na Internet, levando a que um menor fosse alvo de abordagens de pedófilos; a Lei finlandesa em vigor, que visava proteger a liberdade de expressão e o direito à expressão anónima e protegia os autores de mensagens anónimas na *Internet*, impediu as autoridades de ordenarem ao fornecedor de serviços que lhes disponibilizasse metadados que permitissem a identificação do agente da infração, o que votara ao insucesso a investigação.

---

[343] Cfr. Acórdãos McCann e Outros c. Reino Unido, Mahmut Kaya c. Turquia, Hugh Jordan c. Reino Unido, Paul e Audrey Edwards c. Reino Unido, Nachova e Outros c. Bulgária, Kaya e Outros c. Turquia, Ramsahai e Outros c. Países Baixos, Angelova e Iliev c. Bulgária, Opuz c. Turquia, Kolevi c. Bulgária, Al-Skeini e Outros c. Reino Unido, Vasîlka c. Moldávia, Jaloud c. Países Baixos, Mustafa Tunç e Fecire Tunç c. Turquia e Armani da Silva c. Reino Unido.

[344] Cfr. Acórdãos K.U. c. Finlândia, Khadija Ismayilova c. Azerbaijão e Volodina c. Rússia (n.º 2).

6. O Tratado da União Europeia e a Carta dos Direitos Fundamentais da União Europeia vs. a Convenção Europeia dos Direitos Humanos e a Constituição da República Portuguesa

Os Direitos Fundamentais encontram-se consagrados nos arts. 7.º e 8.º da CDFUE e 20.º, n.º 1, 26.º, n.º 1, e 35.º, n.os 1 e 4, da CRP.

Todavia, existem outros direitos fundamentais protegidos pela CDFUE[345] que foram, pura e simplesmente ignorados pelo TJUE, sendo certo que a ponderação de interesses à luz do princípio da proporcionalidade tem de considerar todos os interesses contrapostos, precisamente porque essa ponderação visa obter uma concordância prática entre esses mesmos interesses. Além disso, o princípio da proporcionalidade foi considerado apenas na sua vertente de proibição do excesso, ignorando-se a vertente de proibição de insuficiência desse mesmo princípio[346], sobretudo quando está em causa, entre outras finalidades, "a luta contra a criminalidade grave"[347].

E o TC incorreu na mesma falha, ao também não considerar minimamente (ou se o considerou, tal não resulta do texto do Acórdão n.º 268/2022) os interesses (obviamente legítimos) prosseguidos por via da administração da Justiça penal (onde se inclui a investigação criminal e mesmo

---

[345] De facto, a CDFUE também garante, no seu art. 6.º, os direitos à liberdade e à segurança, bem como, noutros preceitos, diversos direitos fundamentais que constituem o referente constitucional de bens jurídicos tutelados por diversos tipos de crime particularmente graves e cuja prevenção e repressão são essenciais num Estado de Direito, como, por exemplo, os direitos à vida (art. 2.º), à integridade pessoal (art. 3.º), a não ser escravizado nem alvo de redução à servidão ou sujeito a tráfico de seres humanos (art. 5.º), à propriedade (art. 17.º), à saúde (art. 35.º), ao ambiente (art. 37.º), a uma boa Administração (art. 41.º), à ação e a um Tribunal imparcial (art. 47.º), etc., que, na nossa ótica, não foram tidos em conta pelo TJUE. E o mesmo sucede, inclusivamente, com os direitos ao respeito pela vida privada e familiar (art. 7.º) e à proteção de dados pessoais (art. 8.º), que também podem ser lesados por via da prática de crimes, pelo que não podem ser considerados apenas para justificar a limitação da utilização de medidas de investigação criminal.

[346] Acerca do princípio da proporcionalidade na vertente de proibição de insuficiência e da sua aplicação no âmbito do Direito penal e processual penal, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 311 e ss.

[347] A que podemos subsumir a criminalidade organizada, o terrorismo, a criminalidade económico-financeira, a criminalidade violenta e outras formas de criminalidade, como os crimes sexuais (mesmo quando não impliquem o uso de violência e não sejam cometidos para obtenção financiamento do terrorismo e/ou de lucro para grupos criminosos organizados) ou mesmo os crimes puníveis com pena de prisão cujo limite máximo seja superior a 5 anos.

a prevenção criminal *ante delictum*), que visam a proteção dos direitos fundamentais dos cidadãos[348] contra o crime e não o engrandecimento do Estado[349]. E, como sabemos, para que a criminalização de uma conduta seja admissível, terá de estar em causa a proteção de um bem jurídico essencial à convivência comunitária e ao livre desenvolvimento da pessoa, que terá de estar relacionado com um direito fundamental ou com um interesse constitucionalmente protegido, sendo os bens jurídico-penais concretizações dos valores constitucionais expressa ou implicitamente ligados aos direitos e deveres fundamentais e à ordenação social, política e económica[350]; deste modo, no caso dos crimes que integram o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008, está em causa a proteção de alguns dos bens mais relevantes à luz da ordem de valores jurídico-constitucional[351].

Ainda no que tange à CDFUE, há que ter em conta o disposto no seu art. 53.º, nos termos do qual, «*Nenhuma disposição da presente Carta deve ser interpretada no sentido de restringir ou lesar os direitos do Homem e as liberdades fundamentais reconhecidos, nos respetivos âmbitos de aplicação, pelo direito da União, o direito internacional e as Convenções internacionais em que são Partes a União ou todos os Estados-Membros, nomeadamente a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, bem como pelas Constituições dos Estados-Membros*».

---

(348) De resto, o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008, inclui crimes gravíssimos, como sejam: homicídio doloso, ofensa à integridade física grave, mutilação genital feminina, ofensa à integridade física agravada pelo resultado, violência doméstica, violação, coação sexual, abuso sexual de menores, roubo, extorsão, associação criminosa, tráfico de órgãos, tráfico de pessoas, tráfico de armas, tráfico de droga, corrupção, tráfico de influência, participação económica em negócio, branqueamento de capitais, grupo terrorista, terrorismo, financiamento do terrorismo, rapto, sequestro agravado, tomada de reféns, escravidão, tortura, etc. De todo o modo, afigura-se-nos que este catálogo é excessivamente restritivo, não se percebendo, desde logo, porque é que é mais restritivo do que o catálogo dos arts. 187.º, n.º 1, do CP e 18.º, n.º 1, da Lei n.º 109/2009.

(349) Cfr. DUARTE RODRIGUES NUNES, Curso de Direito Processual Penal, 1, p. 147.

(350) Cfr. FIGUEIREDO DIAS, Direito Penal, Parte Geral, Tomo I, 3.ª Edição, pp. 136 e ss., e DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, 2.ª Edição, p. 88.

(351) Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in RMP, n.º 170, p. 33.

Daqui resulta que a aplicação da CDFUE não pode conduzir a uma menor proteção de direitos fundamentais do que a proteção proporcionada por outros instrumentos de Direito internacional (como a CEDH) ou das Constituições dos Estados-Membros.

No caso da CRP, cumpre considerar o art. 8.º, n.º 4, nos termos do qual, as normas do Direito da União Europeia são aplicáveis na ordem jurídica portuguesa nos termos definidos pelo Direito da União Europeia (incluindo a sua interpretação pelo TJUE), *mas sempre com respeito pelos princípios fundamentais do Estado de Direito Democrático,* sendo que esta reserva constitucional prevista na parte final do n.º 4 do art 8.º da CRP, nas palavras de GOMES CANOTILHO/VITAL MOREIRA[352], *«poderá considerar-se como uma norma de colisão explícita, pois ela torna claro que o princípio do primado do direito da União está limitado por núcleo essencial da Constituição – princípios fundamentais do Estado de direito democrático – que funcionarão como uma espécie de «reserva de ordem pública constitucional» («teoria dos contratualistas») contra eventuais preceitos ou disposições do direito da União aniquiladores da estadualidade (Estado), juridicidade (Estado de direito), democraticidade (Estado de direito constitucional) e fundamentalidade de direitos básicos (Estado de direitos fundamentais)».*

No fundo, esta reserva constitucional do art. 8.º, n.º 4, *in fine,* da CRP corresponde *grosso modo* à ressalva contida no art. 53.º da CDFUE.

Ainda no que concerne ao Direito da União Europeia, nos termos do art. 6.º, n.º 2 e 3, da CDFUE (na versão *oficial portuguesa*):

«2. A União adere à Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. Essa adesão não altera as competências da União, tal como definidas nos Tratados.

3. Do direito da União fazem parte, enquanto princípios gerais, os direitos fundamentais tal como os garante a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais e tal como resultam das tradições constitucionais comuns aos Estados-Membros».

[352] GOMES CANOTILHO/VITAL MOREIRA, Constituição Anotada, I, 4.ª Edição, p. 267.

Ainda que, formalmente, a UE não tenha aderido à CEDH e, pelo menos, as versões inglesa e espanhola refiram que a UE "aderirá" e que os direitos fundamentais garantidos pela CEDH "farão parte" do Direito da União Europeia enquanto princípios gerais de direito, pelo menos nas versões portuguesa, italiana, alemã e francesa, refere-se que a UE "adere" e que os direitos fundamentais garantidos pela CEDH "fazem parte" do Direito da União Europeia enquanto princípios gerais de direito. Por isso, do ponto de vista material, tendo em conta, não apenas o art. 6.º, n.os 2 e 3, do TUE, mas sobretudo o art. 53.º da CDFUE, a UE, do ponto de vista material, está vinculada à CEDH e os direitos fundamentais garantidos pela CEDH tal como interpretados pelo TEDH integram o Direito da União Europeia. E não podemos olvidar que os Estados-Membros da UE são igualmente Estados-Membros do Conselho da Europa, estando, por isso, sujeitos à CEDH e à jurisprudência do TEDH.

Deste modo, a CEDH, tal como interpretada pelo TEDH, prevalece sobre a CDFUE e a jurisprudência do TJUE[353], que cedem igualmente perante a CRP nos casos em que esta conceda uma melhor proteção dos direitos fundamentais[354], sendo que a prevenção e a repressão de crimes graves são justificadas e mesmo impostas, no plano jurídico-constitucional, enquanto mecanismos de proteção dos bens jurídico-penais e, consequentemente, de direitos fundamentais[355].

E, como referimos, o TEDH considera que a proteção dos direitos fundamentais inclui o dever de as autoridades levarem a cabo uma investigação efetiva e eficaz (o que inclui a obrigação de utilizar os meios de investigação que, não violando o disposto na CEDH, se mostrem

---

[353] Como resulta dos arts. 6.º, n.os 2 e 3, do TUE e 53.º da CDFUE.

[354] Cfr. arts. 53.º da CDFUE e 8.º, n.º 4, in fine, da CRP.

[355] Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 334 e ss. (sobretudo na p. 336), e voto de vencido do Juiz Schluckebier na Sentença do BVerfG de 02/03/2010.

E, como referimos, os crimes que integram o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 protegem alguns dos bens mais relevantes à luz da ordem de valores jurídico-constitucional (cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, p. 33).

necessários no caso concreto) dos crimes que lesem ou ponham em perigo algum dos direitos fundamentais garantidos pela CEDH, não faltando casos de condenação de Estados por ineficácia da investigação criminal em virtude do não uso de meios investigatórios que se mostrem necessários para investigar os crimes em causa no caso concreto.

7. Apreciação crítica da jurisprudência do Tribunal de Justiça da União Europeia e do Tribunal Constitucional em matéria de conservação e utilização de metadados conservados na investigação criminal

Compulsados os textos dos Acórdãos *Digital Rights* (do TJUE) e n.º 268/2022 (do TC), deparamos, desde logo, com uma grave falha metodológica, que se prende com o facto de, em ambos os arestos, não ter sido realizada qualquer ponderação entre os direitos à intimidade/privacidade e à autodeterminação informacional (ambos os Tribunais) e à tutela jurisdicional efetiva (no caso do TC) e os direitos fundamentais a que se reconduzem os bens jurídicos tutelados pelos crimes constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 (no caso do TC) e pelos crimes subsumíveis ao conceito de criminalidade grave[356] utilizado pelo TJUE (no caso do TJUE)[357].

Contudo, dado que, do outro lado da rua, também está em causa a proteção de direitos fundamentais, impunha-se que o TJUE e o TC tivessem realizado uma ponderação entre os interesses em conflito, não se podendo olvidar que alguns dos direitos fundamentais a que se reconduzem os bens jurídicos tutelados pelos crimes constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 e pelos crimes subsumíveis ao conceito

[356] A que podemos subsumir a criminalidade organizada, o terrorismo, a criminalidade económico-financeira, a criminalidade violenta e outras formas de criminalidade, como os crimes sexuais (mesmo quando não impliquem o uso de violência e não sejam cometidos para obtenção financiamento do terrorismo e/ou de lucro para grupos criminosos organizados) ou mesmo os crimes puníveis com pena de prisão cujo limite máximo seja superior a 5 anos.

[357] A nossa apreciação cinge-se à questão do combate à criminalidade, que inclui a segurança pública (que é a questão que foi tida em conta pelo TC no Acórdão n.º 268/2022), não se considerando a questão da admissibilidade da obtenção de metadados pelos serviços de informações para salvaguarda da segurança nacional (que também tem sido considerada na jurisprudência do TJUE e foi objeto dos Acórdãos do TC n.ºs 403/2015 e 464/2019, em que o TC considerou, e bem, inconstitucionais, normas que previam o acesso, pelos serviços de informações a metadados).

de criminalidade grave integram o elenco dos direitos fundamentais mais relevantes à luz da ordem de valores jurídico-constitucional da CRP e da CDFUE e que direitos como o direito à vida e à integridade pessoal são, inclusivamente, mais valiosos dos que os direitos invocados pelo TJUE para invalidar a Diretiva 2006/24/CE e pelo TC para declarar a inconstitucionalidade dos arts. 4.º, 6.º e 9.º da Lei n.º 109/2009.

Além disso, a ponderação teria sempre de ser levada a cabo *in concreto* (ou seja, considerando a natureza, o âmbito e a intensidade da restrição dos direitos à intimidade/privacidade, à autodeterminação informacional e à tutela jurisdicional efetiva) e não em abstrato (com base numa ideia de ordem hierárquica de valores constitucionais)[358], sendo que, como veremos, as restrições a estes direitos por via da conservação e utilização probatória de metadados conservados, nos casos em que existem efetivamente, são de intensidade pouco significativa.

Não obstante, o TJUE e o TC não realizaram qualquer ponderação de interesses, afigurando-se-nos que, se essa ponderação tivesse sido realizada, o TC jamais teria declarado a inconstitucionalidade dos arts. 4.º, 6.º e 9.º da Lei n.º 109/2009.

Na sua jurisprudência subsequente ao Acórdão *Digital Rights* (relativa à Diretiva 2002/58/CE, conforme alterada pela Diretiva 2009/136/CE)[359], o TJUE passou a fundamentar as decisões numa ponderação de interesses, tendo enunciado os seguintes parâmetros:

a) A CDFUE proíbe a conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica;

---

[358] Cfr. VIEIRA DE ANDRADE, Os Direitos Fundamentais na Constituição Portuguesa de 1976, 3.ª Edição, p. 323, e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 310.

[359] Cfr. Acórdãos Tele2 Sverige AB e Secretary of State for the Home Department, Ministerio Fiscal, Privacy International, La Quadrature du Net, Prokuratuur, G. D. e Commissioner of An Garda Síochána e SpaceNet e Telekom Deutschland.

b) A CDFUE impõe que os dados sejam conservados no território da União Europeia;

c) A CDFUE permite a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização para salvaguarda da segurança nacional, quando o Estado-Membro em causa enfrente uma ameaça grave, real e atual ou previsível[360], desde que essa conservação apenas ocorra durante um período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça, e a decisão que determina a conservação seja efetivamente fiscalizada por um órgão jurisdicional ou por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos;

d) A CDFUE permite a conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, desde que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;

e) A CDFUE permite conservação generalizada e indiferenciada, por um período temporalmente limitado ao estritamente necessário, dos endereços IP atribuídos à fonte de uma ligação, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional;

f) A CDFUE permite conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública; e

---

[360] O que, no caso de Portugal, torna impossível a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, sendo certo que o TJUE apenas admite esta conservação generalizada e indiferenciada para fins de salvaguarda da segurança nacional e não para fins de resposta à criminalidade grave (ainda que algumas formas de criminalidade grave sejam, concomitantemente, ameaças à segurança nacional, como sucede com o terrorismo), o que não se entende.

g) A CDFUE permite o acesso a metadados conservados para efeitos de luta contra a criminalidade grave e desde que esse acesso esteja sujeito a controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente (que não inclui o MP, pois é o titular da ação penal).

O que dizer destas condições impostas pelo TJUE?

Em primeiro lugar, no caso da conservação seletiva, as condições são impossíveis de cumprir e são de difícil (ou mesmo impossível) determinação.

São impossíveis de cumprir porque a conservação de metadados é uma medida de prevenção criminal que se integra na chamada investigação proativa e ocorre, por natureza, num momento prévio à obtenção da notícia do crime, sendo, por isso, impossível definir um qualquer critério delimitador dos metadados a conservar e, ainda que fosse possível, tal critério sempre violaria os princípios da proibição da discriminação e da presunção de inocência.

São de difícil (ou mesmo impossível) determinação, pois, ainda que o TJUE esclareça que a preservação da segurança nacional corresponde ao interesse primordial de proteger as funções essenciais do Estado e os interesses fundamentais da Sociedade, através da prevenção e da repressão de atividades suscetíveis de desestabilizar gravemente as estruturas constitucionais, políticas, económicas ou sociais fundamentais de um país (em especial, ameaçar diretamente a Sociedade, a população ou o Estado), dando o exemplo do terrorismo, fica por saber, por exemplo, se tal também inclui a criminalidade organizada *(maxime as máfias)* e, na afirmativa, se inclui todos os casos de criminalidade organizada mafiosa ou apenas aqueles casos em que as máfias ameacem diretamente o Estado, os seus agentes e os cidadãos de uma forma generalizada (gerando um ambiente generalizado de medo), excluindo as situações em que isso não suceda ou tenha deixado de suceder.

E são de difícil (ou mesmo impossível) determinação também pelo facto de não vermos como é que, com base em elementos objetivos e não discriminatórios (e quais são ou poderão ser esses elementos), em função das categorias de pessoas em causa ou através de um critério geográfico,

será possível definir um qualquer critério delimitador dos metadados a conservar e, sobretudo, fazê-lo sem violar a presunção de inocência e a proibição de discriminação.

Podemos, pois, afirmar, com segurança, que a conservação seletiva dos dados de tráfego e dos dados de localização nos termos propostos pelo TJUE é absolutamente inviável e, por isso, esta (aparente) possibilidade é, na realidade, uma impossibilidade.

Em segundo lugar, na sequência do que referimos, estas exigências abrem a porta a um tratamento discriminatório entre os cidadãos, pois a limitação da conservação de dados em função das categorias de pessoas (*v.g.*, indivíduos com antecedentes criminais ou com antecedentes criminais de uma determinada tipologia, indivíduos oriundos de países ou de regiões conotadas com determinadas atividades criminosas ou que desempenham uma determinada atividade profissional ou económica conotada com certas atividades criminosas) ou de um critério geográfico (*v.g.*, os habitantes de uma determinada região, de uma determinada localidade, de parte de uma localidade ou de um bairro) encerra um enorme risco de discriminação dos visados face aos não visados, inclusivamente no que tange à presunção de inocência e não apenas no que concerne ao tratamento informático de dados relativos à vida privada *ex se*.

Em terceiro lugar, o entendimento do TJUE ignora o facto de a criminalidade organizada, o terrorismo, o cibercrime e a criminalidade económico-financeira serem formas de criminalidade tendencialmente e em muitos casos (porventura na maioria dos casos) transnacional, podendo a atividade criminosa desenvolver-se no território de dois ou mais Estados; e alguns dos Estados em que atividade criminosa é levada a cabo poderão ser Estados não-membros da UE (e, como tal, não sujeitos à jurisprudência do TJUE), mas aos quais o ou os Estados-Membros da UE deva(m) prestar cooperação no âmbito de instrumentos de Direito internacional extracomunitários (*v.g.*, instrumentos de prevenção e repressão da criminalidade adotados no âmbito da ONU ou do Conselho da Europa[361]).

[361] Daí resultando que a jurisprudência do TJUE pode pôr em causa instrumentos de combate à criminalidade adotados no âmbito da ONU ou do Conselho da Europa.

Em quarto lugar, o TJUE também olvida que a atividade criminosa pode ser levada a cabo ou as suas consequências danosas podem verificar-se no Estado A, mas os criminosos utilizarem o Estado B como base de operações ou como ponto de recuo depois do cometimento dos crimes ou praticarem no Estado B os atos preparatórios ou de execução dos crimes cujas consequências se verificam no Estado A; e também olvida que as ações de prevenção criminal relativamente a crimes que virão ou poderão vir a ser cometidos no Estado A podem ter de ser levadas a cabo também no Estado B.

Em quinto lugar, relativamente aos casos em que o TJUE admite a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, não se percebe como é que tal só é admitido para fins de salvaguarda da segurança nacional (ou seja, pelos serviços de informações) e não também para a luta contra a criminalidade grave (ainda que algumas formas de criminalidade grave sejam, concomitantemente, ameaças à segurança nacional, como sucede com o terrorismo).

E, em sexto lugar, relativamente à diferenciação entre os endereços IP atribuídos à fonte de uma ligação (que serão, tendencialmente, dados de base) e os dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (que também são dados de base), não se entende uma tal diferenciação, sobretudo quando, pelo menos à partida, em termos de privacidade, o conhecimento da residência de uma pessoa será mais lesivo do que o conhecimento do IP que está atribuído a um determinado sistema informático e, apesar disso, o TJUE é bastante mais restritivo quanto à admissibilidade da conservação generalizada e indiferenciada dos os endereços IP do que quanto à admissibilidade da conservação generalizada e indiferenciada dos dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos.

Passando ao TC, tendo em conta o que já referimos e o que referiremos infra, o TC não estava obrigado a seguir a jurisprudência do TJUE no Acórdão *Digital Rights*. No entanto, o Acórdão do TC n.º 268/2022 padece de problemas muito mais graves do que a ausência de ponderação entre os direitos à intimidade/privacidade, à autodeterminação informacional e à tutela jurisdicional efetiva e os direitos fundamentais a que se reconduzem os

bens jurídicos tutelados pelos crimes constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008.

Em primeiro lugar, ao contrário do que é afirmado pelo TC (e aqui divergimos do voto de vencido) e pelo TJUE, a mera conservação de metadados não restringe qualquer direito fundamental[362], apenas ocorrendo uma restrição se e quando os dados forem acedidos[363], sendo que a conservação, por si só, não revela quaisquer informações, apenas permitindo o uso futuro de elementos de prova em investigações criminais que, de outro modo, teriam desaparecido e não poderiam ser utilizados, num Estado de Direito, esse aumento da eficácia da investigação só pode ser considerado positivamente[364]. No fundo, tal como sucede na preservação expedita de dados informáticos e na revelação expedita de dados de tráfego previstas nos

---

[362] Dado que, nos termos dos arts. 3.º, n.º 3, e 7.º, n.º 2, da Lei n.º 32/2008, os metadados terão de ser guardados em ficheiros *(que têm de estar obrigatoriamente separados de quaisquer outros ficheiros para outros fins)* e *encriptados* e, nos termos dos arts. 3.º, n.ºs 1 e 2, 8.º e 9.º, n.º 1 (abstraindo do facto de considerarmos que este preceito foi tacitamente revogado pela Lei n.º 109/2009 (cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 557 e ss., e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 65 e ss.), esses ficheiros só podem ser desencriptados e acedidos para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes e mediante despacho judicial fundamentado; isto sem embargo de, por entendermos que o art. 9.º da Lei n.º 32/2008 foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009, a entidade competente para autorizar o acesso aos metadados seja a autoridade judiciária no caso de dados de base e de localização celular (cfr. art. 14.º, n.ºs 1 e 4, da Lei n.º 109/2009) e, no caso dos dados de tráfego, o JIC ou o Juiz (cfr. arts. 18.º, n.º 2, da Lei n.º 109/2009, na fase de inquérito, e 189.º, n.º 2, do CPP, nas demais fases processuais). Aliás, não vemos em que medida a obtenção de dados conservados terá de ser rodeada de maiores garantias do que no caso de esses dados serem obtidos em tempo real.

Além disso, só os funcionários do operador de comunicações eletrónicas que estejam especialmente autorizados para tal poderão aceder aos dados, sob pena de responsabilidade penal (cfr. art. 13.º, n.º 1, al. c), da Lei n.º 32/2008), e a sua identidade tem de ser comunicada à CNPD, sob pena de responsabilidade contraordenacional (cfr. art. 12.º, n.º 1, al. d), da Lei n.º 32/2008).

Ou seja, na fase de conservação, os metadados são, apenas e só, inseridos em ficheiros que ficavam encriptados e intocados até à sua destruição ao fim de 1 ano, a menos que fosse autorizado o acesso a determinados metadados (que seriam apenas os metadados relativos ao arguido, ao suspeito, ao intermediário ou, mediante consentimento, à vítima e não a todos os metadados que estivessem naquele ou naqueles ficheiros) e nada mais.

[363] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, p. 28.

[364] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in RMP, n.º 170, p. 29.

arts. 12.º e 13.º da Lei n.º 109/2009[365], a conservação de metadados não restringe qualquer direito fundamental.

Em segundo lugar, ainda que se admitisse que a mera conservação de metadados restringe direitos fundamentais, tratar-se-ia de uma restrição pouco intensa[366].

De resto, como vimos, o TEDH tem considerado que a proteção dos direitos fundamentais inclui o dever de as autoridades levarem a cabo uma investigação efetiva e eficaz (o que inclui a obrigação de utilizar os meios de investigação que, não violando o disposto na CEDH, se mostrem necessários no caso concreto) dos crimes que lesem ou ponham em perigo algum dos direitos fundamentais garantidos pela CEDH.

[365] Cfr. DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 84-84 e 101.

[366] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, p. 30.

De resto, no que tange aos dados de base, o próprio TC, no Acórdão n.º 268/2022, considera que se trata de uma restrição pouco intensa.

No caso dos dados de localização, a única informação que esses dados fornecem é a localização de um determinado dispositivo, a partir da qual se vai *inferir* (de forma ilidível) que o seu proprietário ou utilizador habitual se encontra nesse mesmo local, sendo incorreto afirmar que os dados de localização permitem saber a localização de uma pessoa; por isso, a obtenção (e não a conservação, que não revela quaisquer dados) de dados de localização celular constitui uma restrição pouco intensa de direitos fundamentais (cfr. DUARTE RODRIGUES NUNES, "Da admissibilidade da obtenção de dados de localização celular ou de dados de tráfego de todos os telemóveis/cartões que acionaram um determinado conjunto de antenas/células de telecomunicações no lapso de tempo em que o crime sob investigação terá sido praticado, para posterior identificação dos seus autores", in *RMP*, n.º 157, p. 133, Acórdãos do TC n.º 486/2009 e do STJ de 29/04/2010 e Sentenças do BGH de 24/01/2001 e do *Tribunal Supremo* n.º 6307/2009; contra, Acórdão do TC n.º 268/2022 e Sentença *United States v. Jones do Supreme Court of the United States).*

Por fim, no caso dos dados de tráfego, trata-se dos elementos ou dados funcionais necessários ou produzidos pelo estabelecimento da ligação através da qual uma comunicação concreta é operada ou transmitida [a direção, o destino *(adressage)* e a via, o trajeto *(routage)*], os quais se limitam a revelar – no caso de comunicações telefónicas – os números das chamadas recebidas e os números para os quais aquele dispositivo ligou (daí se *inferindo,* uma vez mais de forma ilidível, que as comunicações tiveram lugar entre os proprietários ou os utilizadores habituais de cada um desses números telefónicos) e a data, a duração, a hora, e a frequência dessas comunicações ou tentativas de comunicação e nada mais, pois nada revelam quanto ao conteúdo das comunicações; por isso, trata-se de uma restrição também pouco intensa de direitos fundamentais e que, por ser muito menos intensa do que no caso da obtenção de dados de conteúdo, a sua obtenção, ainda que restrinja o direito à inviolabilidade das comunicações, nem deveria estar sujeita ao regime particularmente restritivo das interceções de comunicações (cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 577), como sucede no Direito alemão (em que o legislador consagrou, no §100g da StPO, um regime muito menos restritivo do que o das interceções de comunicações do §100a).

Em terceiro lugar, a conservação e os ulteriores acesso e utilização de metadados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes (*cfr.* art. 3.º, n.º 1, da Lei n.º 32/2008), o que inclui a repressão criminal e a prevenção criminal, tendo em conta o *continuum* que existe (e terá de existir[367]) entre ambas como *conditio sine qua non* para responder eficazmente à criminalidade organizada, ao terrorismo, à criminalidade económico-financeira e ao cibercrime[368]. E, como referimos, o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008[369] inclui crimes gravíssimos, cujos bens jurídicos protegidos têm como referente constitucional alguns dos bens mais relevantes à luz da ordem de valores jurídico-constitucional.

Ora, a utilização de metadados tende a ser absolutamente essencial para muitas investigações criminais desses tipos de crime (e de outros), *maxime* quando se trate de formas de criminalidade que utilizam sistematicamente meios informáticos e/ou outros meios eletrónicos de comunicação à distância (designadamente, a criminalidade organizada, o terrorismo, a criminalidade económico-financeira ou o cibercrime[370] *ex se*) cuja utilização

---

Reconhecemos, porém, que a intensidade da restrição poderá ser mais intensa – embora sem que possa ser comparada à obtenção de dados de conteúdo de comunicações por via da interceção de comunicações – no caso dos dados de tráfego relativos à navegação na Internet, ainda que, também aqui, apenas se obtenham as informações relativas às páginas de *Internet* "visitadas" por via daquele sistema informático, inferindo-se, a partir daí (de forma ilidível), que foi o proprietário ou utilizador habitual desse sistema informático quem acedeu a essas páginas (e, por isso, a restrição também não pode ser qualificada como intensa).

(367) Sobre esse continuum, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 255 e ss.

(368) Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 581, e também em "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, p. 32.

(369) Embora consideremos que a obtenção de dados de localização ou de base não está sujeita a qualquer catálogo de crimes (cfr. art. 14.º da Lei n.º 109/2009) e que a obtenção de dados de tráfego está sujeita ao catálogo do art. 18.º, n.º 1, da Lei n.º 109/2009, que é mais amplo do que o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008.

(370) Que, quando entendido em sentido lato (tal como defendemos), inclui tanto os crimes em que o sistema informático ou os dados informáticos são o objeto da ação, ainda que como alvos simbólicos (cibercrime em sentido estrito) como outros crimes cujo cometimento esteja significativamente ligado à utilização

gera metadados[371]. E, como é óbvio, a notícia do crime é sempre obtida após a prática do crime (e, não poucas vezes, muito depois) e, mesmo quando o processo é instaurado pouco tempo após a prática do crime, muitas vezes, a identificação de arguidos ou suspeitos só ocorre muito tempo depois da instauração do processo (e só aí é que a obtenção de metadados relativos ao suspeito, ao arguido ou ao intermediário será possível e admissível)[372]. Por isso, os metadados que interessa obter são metadados gerados no passado e não no decurso da investigação, sendo essa situação que o legislador pretendeu acautelar ao impor a conservação dos metadados através da Lei n.º 32/2008 e o mesmo sucedendo com o Parlamento Europeu e o Conselho ao adotarem a Diretiva 2006/24/CE[373].

Tendo em conta o que acabámos de referir, além de a mera conservação de metadados não restringir direitos fundamentais e de o acesso aos metadados apenas constituir uma restrição de direitos fundamentais que não pode ser considerada intensa, a desconsideração[374] da necessidade de investigar eficazmente os crimes graves constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 configura uma proteção insuficiente dos direitos fundamentais que se concretizam nos bens jurídico-penais tutelados por esses

---

de um sistema informático (onde se incluem, por exemplo, a pornografia infantil, a extorsão sexual, o tráfico de drogas ou armas, o jogo ilícito online, as burlas relativas a criptomoedas, etc.) (cfr. DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 45-46).

(371) Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, pp. 33-34.

(372) Assim, DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, p. 34.

(373) Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, p. 34.

(374) Ao ponto de ocorrer um sacrifício a cem por cento do valor da segurança (cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, p. 34, e voto de vencido do Acórdão do TC n.º 268/2022) e dos demais direitos fundamentais que se concretizam nos bens jurídico-penais tutelados pelos crimes constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 (cfr. DUARTE RODRIGUES NUNES, *Idem*, pp. 34-35).

crimes[375], sendo que a Lei n.º 32/2008 encontrara um equilíbrio que proporcionava uma muito adequada concordância prática entre os valores em colisão[376]. Aliás, atentas a natureza dos crimes que integram o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008, a intensidade da restrição de direitos fundamentais que o acesso e a utilização dos metadados acarretam e as salvaguardas que o legislador previra na Lei n.º 32/2008, os direitos ou interesses constitucionalmente protegidos prosseguidos através da investigação criminal tendem a ser mais relevantes à luz da ordem de valores jurídico-constitucional do que os direitos fundamentais restringidos, o que foi completamente ignorado pelo TC[377]. E não podemos olvidar que o interesse público numa Justiça penal funcionalmente eficaz é um pressuposto essencial do Estado de Direito e possui, também ele, respaldo constitucional[378], sendo que a investigação dos crimes e a punição dos criminosos é levada a cabo em prol do interesse da Comunidade no seu todo e não em prol do engrandecimento do Estado[379].

Em quarto lugar, como se afirma no voto de vencido, se só for possível conservar metadados relativamente a pessoas em relação às quais existam indícios de que o seu comportamento possa ter algum nexo com os crimes graves enunciados na al. g) do n.º 1 do art. 2.º da Lei n.º 32/2008, os fornecedores de serviços de telecomunicações apenas poderão conservar

---

(375) Como resulta da jurisprudência do TEDH que referimos.

(376) Como se aduz no voto de vencido do Acórdão do TC n.º 268/2022.

(377) Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in RMP, n.º 170, p. 35.

(378) Cfr. FIGUEIREDO DIAS, Acordos Sobre a Sentença em Processo Penal, pp. 37 e ss., DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 335 e ss., e também em Curso de Direito Processual Penal, 1, p. 147, CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", in *RMP,* n.º 139, p. 39 (nota 21), Acórdãos Paul e Audrey Edwards c. Reino Unido do TEDH, do TC n.º 213/2008, do STJ de 03/03/2010 e da RL de 24/01/2012 e Sentenças do BVerfG de 27/06/2018, National City Trading Corp. v. United States do *United States Court of Appeals, 2nd Circuit* (1980) e United States v. Hunter do *United States District Court, Vermont* (1998).

(379) Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP,* n.º 170, p. 35.

os dados quando a autoridade judiciária competente os solicitar no decurso de uma investigação criminal, situação que já está prevista no art. 12.º da Lei n.º 109/2009 (cuja aplicação depende de os dados a preservar terem sido previamente conservados[380]), mas que poderá ser insuficiente para o apuramento da verdade e para a efetiva recolha de prova[381].

Em quinto lugar, apesar de a Lei n.º 32/2008 ser o diploma através do qual o legislador transpôs a Diretiva 2006/24/CE para o Direito português, a declaração de invalidade da Diretiva não implica por si só a invalidade da Lei n.º 32/2008 à luz do Direito União Europeia, pois a conservação e a obtenção de registos da realização de comunicações e de dados de localização não dependem, ex se, dessa Diretiva, nada impedindo a sua consagração legal na falta de uma tal Diretiva[382]. Ademais, o legislador nacional criou um quadro normativo que vai muito para além da Diretiva ao prever um regime jurídico que cumpre as exigências cuja inobservância pela Diretiva levou o TJUE a declarar a invalidade da Diretiva não sejam aplicáveis à Lei n.º 32/2008[383].

Em sexto lugar, permitindo a Lei que os prestadores de serviços de comunicações eletrónicas conservem, pelo prazo de seis meses, uma grande parte dos metadados incluídos no art. 4.º da Lei n.º 32/2008 para efeitos de faturação (*cfr.* arts. 6.º, n.º 3, e 7.º da Lei 41/2004, de 18 de agosto, e 9.º,

---

(380) No mesmo sentido, DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, p. 36 (nota 38), e RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", in *RMP*, n.º 172, p. 38.

(381) Por exemplo, numa situação de rapto, se os dados relativos às comunicações das vítimas não forem conservados, poderá ser muito difícil identificar os agentes dos crimes, uma vez que os metadados que vierem a ser obtidos em tempo real serão tendencialmente inúteis, dado que os telefones das vítimas terão sido certamente deixados no local onde o rapto ocorreu, para impedir a sua monitorização pelas autoridades.

(382) Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 559.

(383) Relativamente às razões porque entendemos que os fundamentos que levaram o TJUE a declarar a invalidade da Diretiva não são aplicáveis à Lei n.º 32/2008, vide DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 559 e ss.

n.º 2 e 10.º. n.º 1, da Lei n.º 23/96 de 26 de julho)[384], não se pode conceber que o interesse privado das operadoras cobrarem os serviços prestados aos seus clientes possa ser mais relevante do que o interesse público numa Justiça penal funcionalmente eficaz, sobretudo quando se trate da investigação de crimes que atentam contra os valores mais eminentes da ordem de valores jurídico-constitucional (como sucede com a vida e/ou a integridade pessoal, que a CRP reputa como invioláveis), ao ponto de se admitir como constitucionalmente admissível a conservação de dados para efeitos de faturação e o mesmo já não suceder no caso de conservação para fins de investigação criminal[385].

Em sétimo lugar, no que diz respeito à não previsão da obrigatoriedade de os dados serem conservados num Estado-Membro da União Europeia, como se aduz no voto de vencido, é um problema que nem sequer se deveria colocar, pois o art. 7.º, n.º 4, da Lei n.º 32/2008 remete para as Leis n.os 67/98, de 26 de outubro (sendo que, atualmente, a questão está regulada nos arts. 44.º e ss. do *RGPD*), e 41/2004, de 18 de agosto, onde se resolve a questão da territorialidade e da transferência dentro e para fora da União Europeia (o que torna desnecessária a repetição dessa regulação na Lei n.º 32/2008) e, além disso, quando a Lei sujeita a conservação dos dados ao controlo da CNPD, está a impor, implicitamente, que os dados sejam conservados no território português[386].

Em oitavo lugar, as provas que os metadados podem proporcionar tanto podem servir para provar a prática de crimes pelo arguido como para este

---

[384] E sem que isso ponha em causa a privacidade dos utilizadores, ao ponto de não ter sido também peticionada a declaração da inconstitucionalidade das normas que permitem a conservação para efeitos de faturação, ao contrário do que sucedeu relativamente aos arts. 4.º e 6.º da Lei n.º 32/2008.

[385] Cfr. DUARTE RODRIGUES NUNES/PAULO PINTO DE ALBUQUERQUE, "NOTA PRÉVIA ao Artigo 189.º", in *Comentário do Código de Processo Penal*, Vol. I, 5.ª Edição, pp. 859-860, DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, p. 39, e voto de vencido no Acórdão n.º 268/2022.

[386] DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, p. 40.

demonstrar a sua inocência ou, no mínimo, fazer surgir no julgador uma dúvida razoável, pelo que também a defesa (e não apenas a acusação) fica impossibilitada de utilizar tais provas, que também poderão impedir condenações insustentável e materialmente injustas[387].

Em nono lugar, no que diz respeito à não notificação dos titulares dos dados de que os seus dados foram acedidos pelas autoridades, na maioria das situações, essa notificação é desnecessária e redundante, dado que os dados que foram acedidos são os dados do arguido, que, tendo acesso aos autos, terá perfeito conhecimento de que os seus dados foram acedidos e poderá exercer os seus direitos a esse respeito. Além disso, como se refere no voto de vencido, o art. 9.º da Lei n.º 32/2008 nem sequer é o preceito em que a obrigação da notificação do titular dos dados acedidos deveria constar, pelo que declarar a inconstitucionalidade deste preceito com um tal fundamento não faz qualquer sentido. Ademais, é manifestamente excessivo e desrazoável declarar a inconstitucionalidade de uma norma e, com isso, vedar o recurso a um meio de obtenção de prova absolutamente essencial para investigar crimes graves (na medida em que permite a obtenção de um meio de prova essencial para essa finalidade[388]), com um tal fundamento, sobretudo tendo em conta as consequências jurídicas que poderão advir de uma tal decisão[389].

---

[387] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, p. 41.

[388] Como refere RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", in *RMP*, n.º 172, pp. 34-35, os metadados são um meio de prova, *in casu,* documental (e não um meio de obtenção de prova), que «*podem estar inscritos numa factura detalhada que seja enviada por correio físico ou electrónico para o domicílio do seu titular; podem ser registados através de intercepção das comunicações telefónicas ou de dados informáticos (cf. infra); alguns podem ser encontrados nos sistemas informáticos utilizados nas comunicações; podem estar conservados pelos FS* [fornecedores desses serviços]».

[389] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP,* n.º 170, p. 41.

Em décimo lugar, o entendimento do TC (na esteira do jurisprudência do TJUE), ao poder comprometer seriamente (ou mesmo impossibilitar) muitas investigações criminais de crimes graves ou de formas de criminalidade extremamente danosas e perigosas para os direitos fundamentais dos cidadãos e para a própria subsistência do Estado de Direito – sendo, por isso, violador da CEDH –, poderá conduzir a condenações do Estado Português no TEDH e no pagamento de indemnizações às vítimas, por responsabilidade civil no exercício da função jurisdicional.

Em décimo primeiro lugar, o TC, ainda que reconhecendo que não é possível configurar medidas com a mesma eficácia que a conservação de todos os dados de todas as pessoas, considerou que a conservação de metadados só será legítima se, como entendeu o TJUE, for limitada a dados de localização e de tráfego relativos a um período temporal e/ou a uma zona geográfica determinada e/ou um círculo de pessoas determinado (*in casu,* pessoas que possam estar envolvidas de alguma forma numa infração grave e/ou pessoas que, por outros motivos, a conservação dos seus dados possa contribuir para a luta contra a criminalidade grave), o que levanta, desde logo, dois problemas.

O primeiro desses problemas (porventura o mais grave) é que a limitação da conservação de metadados em função de categorias de pessoas (*v.g.*, indivíduos com antecedentes criminais ou com antecedentes criminais de uma determinada tipologia, indivíduos oriundos de países ou de regiões conotadas com determinadas atividades criminosas ou que desempenham uma determinada atividade profissional ou económica conotada com certas atividades criminosas) ou de um critério geográfico (*v.g.,* os habitantes de uma determinada região, de uma determinada localidade, de parte de uma localidade ou de um bairro) constitui um tratamento discriminatório. Na verdade, como se afirma no voto de vencido, a conservação preventiva de dados geograficamente condicionada, dirigida a um círculo de pessoas determinadas e sem qualquer facto típico cometido não é tolerada pela norma do n.º 3 do art. 35.º da CRP, que apenas admite que o legislador autorize o tratamento informático de dados relativos à vida privada «*com garantias de não discriminação*» e, por isso, o acolhimento,

nesta parte, da jurisprudência do TJUE viola, inclusivamente o disposto nos arts. 8.º, n.º 4, *in fine,* da CRP e 53.º da CDFUE, residindo aqui o primeiro fundamento da inconstitucionalidade do próprio juízo de inconstitucionalidade formulado pelo TC no Acórdão n.º 268/2022.

Mas, esse juízo de inconstitucionalidade também viola o princípio da presunção de inocência, uma vez que a conservação preventiva de dados que vise apenas um círculo de pessoas determinadas e sem qualquer facto típico cometido, pela natureza das coisas, pressupõe uma suspeita de que aquele ou aqueles concretos visados poderão ter cometido ou vir a cometer crimes de que nem sequer existe notícia. E tal situação não tem comparação com a recolha de ADN (argumento que também é utilizado pelo TC), pois a recolha de ADN a condenados é uma consequência jurídica da condenação (que está, de resto, limitada aos casos de maior gravidade e/ou perigosidade[390]) e, ao passo que o ADN é imutável, o condenado pode sempre mudar de dispositivo (telefone, *tablet,* computador), de número de telefone ou de IP ou deixar de os utilizar para o cometimento de crimes (pois sabe que iriam ser monitorizados), tornando a conservação de dados de tráfego e de localização completamente inútil.

Ainda relativamente à presunção de inocência, nem se diga que a conservação generalizada e indiscriminada de metadados constitui uma presunção de culpa ou uma suspeita generalizada sobre todos os cidadãos, uma vez que, como referimos, os metadados são guardados em ficheiros informáticos encriptados e separados de todos os demais ficheiros e só poderão ser desencriptados e acedidos os metadados que disserem respeito ao arguido, ao suspeito, ao intermediário ou à vítima (e, neste caso, apenas mediante consentimento) – e não os metadados de todo e qualquer cidadão –, exclusivamente para a investigação, deteção e repressão de crimes graves

(390) Pois a Lei exige que o visado tenha sido condenado com pena igual ou superior a 3 anos de prisão, ainda que substituída, ou alvo da aplicação de medida de segurança de internamento de inimputáveis, ainda que suspensa na sua execução (cfr. art. 8.º, n.ºs 2 e 3, da Lei n.º 5/2008, de 12 de fevereiro (acerca da obrigatoriedade e da automaticidade da recolha de ADN em arguidos condenados, *vide* DUARTE RODRIGUES NUNES/PAULO PINTO DE ALBUQUERQUE, "Artigo 172.º", in *Comentário do Código de Processo Penal,* Vol. I, 5.ª Edição, pp. 731 e ss.).

por parte das autoridades competentes e mediante despacho fundamentado; e acresce que a utilização de metadados conservados pode inclusivamente ter lugar no interesse do respetivo titular, designadamente quando seja a vítima do crime ou quando, sendo arguido ou suspeito, os metadados possam demonstrar a sua inocência ou, no mínimo, gerar uma dúvida razoável quanto à sua culpabilidade[391].

O segundo problema prende-se com a inexequibilidade/inviabilidade da exigência de que a conservação de metadados seja limitada aos dados relativos a pessoas que possam estar envolvidas de alguma forma numa infração grave e/ou a pessoas cujos metadados, se conservados, possam contribuir, por outras razões (diversas do envolvimento numa infração grave), para a luta contra a criminalidade grave. E é inexequível/inviável, uma vez que a conservação de metadados a que se refere a Lei n.º 32/2008 é uma medida de prevenção criminal que se integra na chamada investigação proativa (que é essencial para responder às novas formas de criminalidade, em que uma investigação meramente reativa, *i.e.,* apenas a partir da obtenção da notícia do crime, é manifestamente ineficaz), sendo que a investigação proativa inicia-se num momento prévio à prática do crime ou ao conhecimento da sua prática pelas autoridades e visa, entre outras finalidades, obter uma *notitia criminis,* obter informações que facilitem a investigação de crimes que venham a ser cometidos[392] ou relativas ao modo de funcionamento de certas formas de criminalidade[393] (as chamadas informações de *intelligence*) ou evitar o cometimento de crimes já planeados ou minimizar os seus efeitos para as vítimas[394].

---

[391] Porquanto, *de jure condito,* as proibições de prova, salvo no caso específico do art. 126.º, n.º 4, do CPP, tornam as provas nulas e inutilizáveis, independentemente de favorecerem a acusação ou a defesa (cfr. DUARTE RODRIGUES NUNES, Curso de Direito Processual Penal, 1, p. 571).

[392] Como também sucede no caso dos deveres de colaboração/reporte ao abrigo da Lei n.º 83/2017, de 18 de agosto, em matéria de combate ao branqueamento de capitais e ao financiamento do terrorismo, e no caso da recolha de ADN de arguidos condenados, nos termos do art. 8.º, n.ºs 2 e 3, da Lei n.º 5/2008, de 12 de fevereiro.

[393] Que também visam simplificar o combate a essas formas de criminalidade no futuro, como sucedeu, por exemplo, nos Estados Unidos e na Itália, em que as autoridades só lograram responder eficazmente à criminalidade organizada de tipo mafioso quando obtiveram informações (na maior parte dos casos, fornecidas por "arrependidos") acerca do chamado "método mafioso" (*i.e., o modus operandi* da máfia).

[394] Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 256-257.

Dito de outro modo, num momento prévio à obtenção da notícia do crime é *impossível* delimitar o âmbito dos metadados a conservar nos termos pretendidos pelo TC (e também pelo TJUE). No fundo, o TC (e o TJUE) formulou uma exigência que é de observância impossível e que contradiz a natureza preventiva, proativa da conservação de metadados e, com isso, declarou a inconstitucionalidade dos arts. 4.º e 6.º da Lei n.º 32/2008, negando, na prática – salvo se for possível encontrar vias alternativas no Direito vigente[395] – a possibilidade de utilização de metadados na investigação criminal, que é um meio absolutamente e cada vez mais necessário para responder às mais graves formas de criminalidade da atualidade.

E, por fim, o juízo de inconstitucionalidade formulado pelo TC no Acórdão do n.º 268/2022 é inconstitucional também por uma outra razão.

Com efeito, o decidido pelo TC, no caso de não ser possível encontrar vias alternativas aos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008 no Direito vigente para obter metadados para as investigações criminais (o que, como referimos, está longe de ser

E, por fim, o juízo de inconstitucionalidade formulado pelo TC no Acórdão do n.º 268/2022 é inconstitucional também por uma outra razão.

Com efeito, o decidido pelo TC, no caso de não ser possível encontrar vias alternativas aos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008 no Direito vigente para obter metadados para as investigações criminais (o que, como referimos, está longe de ser pacífico), pode ter (como já está a ter[396]) consequências devastadoras para a resposta à criminalidade (e, como tal, para a proteção dos direitos fundamentais dos cidadãos[397]), para o restabelecimento da paz jurídica e para a credibilidade da Justiça e do próprio Estado de Direito,

---

[395] O que está longe de ser pacífico entre nós, como é demonstrado pelo levantamento de jurisprudência que realizámos supra.

[396] Veja-se, por exemplo, o sucedido quanto ao processo relativo ao assalto ao paiol de armas de Tancos, em que o Tribunal da Relação de Évora anulou o acórdão do Tribunal de 1.ª Instância por força da valoração de metadados que haviam sido conservados, obrigando à prolação de uma nova decisão que não considere as provas relativas aos metadados (cfr. Acórdão da RE de 28/02/2023).

[397] Pois a prática de crimes também constitui um atentado contra os direitos fundamentais dos cidadãos em geral e das vítimas em particular.

uma vez que:

a) Nos processos em curso, não poderão ser obtidos metadados conservados e aqueles que tiverem sido obtidos não poderão ser usados como prova, o que pode comprometer de sobremaneira a eficácia das investigações e conduzir a decisões absolutórias[398] materialmente injustas, bem como, na medida em que também a defesa fica impossibilitada de os usar, conduzir a decisões condenatórias materialmente injustas; e

b) No caso de condenações transitadas em julgado (sobretudo no caso de crimes graves, de criminosos perigosos e/ou de condenações em penas de prisão efetiva), existe o risco[399] de, nos processos em que os metadados tenham sido decisivos para a condenação[400], indivíduos que comprovadamente cometeram crimes (e, por isso, foram condenados) acabarem por ser absolvidos, com tudo o que isso possa acarretar em termos de prevenção geral e especial, para as vítimas do crime (que poderão vir a ser confrontadas com a absolvição de criminosos que haviam efetivamente cometido crimes contra si e que haviam sido condenados com trânsito em julgado) e, em última análise, para a credibilidade da Justiça e do Estado de Direito aos olhos dos cidadãos; e, mesmo no caso do condenado, as provas que os metadados podem proporcionar também podem servir para, em sede de recurso de revisão, suscitar uma dúvida fundada quanto à justiça da sua condenação[401].

---

[398] Nas "decisões absolutórias" devemos incluir, além das sentenças absolutórias, os despachos de arquivamento (no inquérito) e os despachos de não pronúncia (na instrução).

[399] Embora as condenações transitadas em julgado só possam ser postas em causa por via da interposição de um recurso extraordinário de revisão e o STJ, como vimos, tenha negado, até ao momento, provimento a todos os recursos de revisão interpostos com este fundamento, esse risco não está totalmente afastado, pois as decisões do STJ são passíveis de recurso de constitucionalidade e a própria jurisprudência do STJ pode sofrer alteração.

[400] Designadamente nas situações em que tenha sido através dos metadados que foi possível identificar os suspeitos ou um determinado círculo de suspeitos (e, desse modo, dirigir a investigação para esses indivíduos) e/ou obter as provas que sustentaram a condenação (sendo que dificilmente teria sido possível descobrir/obter sem a prévia obtenção dos metadados) ou em que, no caso de condenações com base em prova indiciária, tenham sido os metadados que permitiram retirar dos indícios a prova dos factos constitutivos do crime.

[401] *V.g.*, os metadados relativos ao arguido A no processo X (e que não eram conhecidos no processo Z, pois o arguido A jamais fora arguido, suspeito, intermediário ou vítima) podem levar ao surgimento de dúvidas fundadas quanto à justiça da condenação de B no processo Z.

Deste modo, o entendimento do TC no Acórdão n.º 268/2022 é também incompatível com o princípio da proporcionalidade (e, como tal, inconstitucional), que não possui apenas uma vertente de proibição do excesso *(Übermaßverbot)*, possuindo igualmente uma vertente de proibição de insuficiência *(Untermaßverbot)*, que é violada quando as entidades (designadamente, o Estado em todas as suas funções: legislativa, jurisdicional e administrativa) oneradas com um dever de proteção *(Schutzpflicht)* não adotam medidas ou adotam medidas insuficientes para garantir uma proteção constitucionalmente adequada dos direitos fundamentais(402), aí se incluindo, por exemplo, a adoção de medidas inadequadas ou ineficazes, o não aperfeiçoamento das medidas existentes, a adoção de medidas que desprotejam os cidadãos face às ameaças ou agressões provenientes de outros cidadãos e a "anulação" de medidas existentes de que resulte uma proteção insuficiente de direitos fundamentais(403). E a proibição de insuficiência vale também no plano do Direito penal (e processual penal)(404), sendo que, como bem afirma ISENSEE(405), o cumprimento do dever estatal de proteção da segurança dos cidadãos tanto poderá consistir na adoção de medidas repressivas como de medidas preventivas.

---

(402) Assim, GOMES CANOTILHO, Direito Constitucional e Teoria da Constituição, p. 273, segundo o qual, ocorre um defeito de proteção (e, como tal, uma violação *Untermassverbot) «quando as entidades sobre quem recai um dever de proteção (Schutzpflicht) adoptam medidas insuficientes para garantir uma proteção constitucionalmente adequada dos direitos fundamentais».*

(403) Cfr. ISENSEE, Das Grundrecht auf Sicherheit, p. 40, JOSÉ PAULO BALTAZAR JÚNIOR, Crime Organizado e Proibição de Insuficiência, p. 68, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 322, HAIN, "Der Gesetzgeber in der Klemme zwischen Übermass – und Untermassverbot", in *DVBl,* 1993, p. 983, UNRUH, Zur Dogmatik der grundrechtlichen Schutzpflichten, pp. 24-25, e PIETRZAK, "Die Schutzpflicht im verfassungsrechtlichen Kontext – Überblick und neue Aspekte", in *JuS*, 1994, pp. 750 e 752-753.

(404) Acerca dos corolários do princípio da proporcionalidade na vertente de proibição de insuficiência e dos deveres estatais de proteção ao nível do Direito penal (em sentido amplo), *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 330 e ss., com vastas referências doutrinárias e jurisprudenciais.

(405) ISENSEE, "§ 111.Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht", in *Handbuch des Staatsrechts der Bundesrepublik Deutschland,* V, 2.ª Edição, p. 218.

É evidente que a proibição de insuficiência não pode ser radicalizada, sob pena de ultrapassagem dos limites de facto e direito a que o legislador está adstrito numa Sociedade livre e democrática[406], mas também não pode ser desvalorizada ao ponto de a esvaziar ou quase esvaziar de efeito útil em favor da proibição do excesso, jamais se podendo afirmar que a proibição de insuficiência apenas vale na medida do possível[407].

A proibição de insuficiência corresponde ao patamar mínimo de proteção do direito fundamental, ao passo que a proibição do excesso corresponde ao patamar máximo admissível da restrição, vigorando a liberdade de conformação do legislador (que define o "como" da proteção dos direitos fundamentais dos cidadãos face a ameaças ou a agressões provenientes de terceiros) no espaço que medeia entre o patamar mínimo de proteção e o limite máximo da restrição[408].

Na medida em que, no momento da aplicação ao caso concreto, ambas as vertentes do princípio da proporcionalidade poderão colidir entre si, haverá que compatibilizá-las, encontrando a proibição de insuficiência limites na proibição do excesso e vice-versa, pois a violação da proibição de insuficiência também pode resultar de uma incorreta aplicação da proibição do excesso e vice-versa[409].

Em suma, o entendimento perfilhado no Acórdão do TC n.º 268/2022 é ele próprio inconstitucional, porquanto dele resulta uma proteção insuficiente dos direitos fundamentais que se concretizam nos bens jurídico-penais

---

(406) Cfr. VIEIRA DE ANDRADE, Os Direitos Fundamentais na Constituição Portuguesa de 1976, 3.ª Edição, p. 149, ISENSEE, "§ 111.Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht", in *Handbuch des Staatsrechts der Bundesrepublik Deutschland,* V, 2.ª Edição, p. 155, e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 325.

(407) Como faz VIEIRA DE ANDRADE, Os Direitos Fundamentais na Constituição Portuguesa de 1976, 3.ª Edição, p. 149 [sobre a nossa crítica a esta afirmação, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 330 (nota 1269)].

(408) Neste sentido, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 328.

(409) Assim, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 328-329.

tutelados pelos crimes constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 ao impossibilitar a conservação e o acesso a esses dados nos termos dos arts. 4.º, 6.º e 9.º dessa Lei, quando:

a) a conservação de metadados, sobretudo tendo em conta o modo como os mesmos são armazenados nos termos da lei, não restringe qualquer direito fundamental;

b) ainda que o acesso aos metadados restringisse direitos fundamentais, fá-lo-ia sempre de uma forma pouco intensa (pelas razões sobreditas), jamais justificando a proteção desses direitos fundamentais (para mais quando são alvo de uma restrição pouco intensa) a completa desconsideração das necessidades de resposta eficaz aos crimes graves constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 e de proteção dos direitos fundamentais protegidos por via da criminalização dessas condutas;

c) assenta em exigências impossíveis de cumprir em face da natureza preventiva da conservação de metadados e cujo (inevitável) incumprimento é utilizado como fundamento para declarar a inconstitucionalidade;

d) é manifestamente excessivo declarar a inconstitucionalidade de uma norma e, com isso, vedar o recurso a um meio de obtenção de prova absolutamente essencial para investigar crimes graves (e para o arguido demonstrar a sua inocência ou, no mínimo, fazer surgir no julgador uma dúvida razoável) com fundamento em essa norma não prever a obrigatoriedade da notificação dos titulares dos dados de que os seus dados foram acedidos pelas autoridades quando, pela sua natureza, não caberia a essa norma regular uma tal matéria e, na maioria das situações, essa notificação é desnecessária e redundante, dado que os dados acedidos são os dados dos arguidos, que, tendo acesso aos autos, têm conhecimento de que os seus dados foram acedidos e poderão exercer os seus direitos a esse respeito; e

e) irá dificultar de sobremaneira a resposta à criminalidade grave ao impedir – caso não seja possível encontrar no Direito vigente uma via alternativa, o que está longe de ser pacífico – a conservação preventiva

dos metadados e a sua utilização probatória nos processos em curso e, no caso de condenações transitadas em julgado, poderá abrir a porta a insustentáveis situações de impunidade com a absolvição de criminosos que haviam sido condenados por sentenças transitadas em julgado.

Ademais, como referimos, o entendimento do TC viola igualmente o princípio da não discriminação no tratamento de dados pessoais (arts. 35.º, n.º 3, da CRP, 14.º da CEDH e 21.º, n.º 1, da CDFUE), o princípio da presunção da inocência (arts. 32.º, n.º 2, 1.ª parte, da CRP, 6.º, §2.º, da CEDH e 48.º, n.º 1, da CDFUE), o disposto nos arts. 8.º, n.º 4, in fine, da CRP e 53.º da CDFUE e, no caso de o arguido/condenado ser impossibilitado de demonstrar a sua inocência ou de gerar uma dúvida razoável acerca da sua culpabilidade ou da justiça da sua condenação, o entendimento do TC viola igualmente o princípio do processo equitativo (*cfr.* arts. 32.º, n.º 1, da CRP, 6.º da CEDH e 47.º da CDFUE).

E reiteramos que a impossibilidade de conservação e de utilizabilidade probatória de metadados conservados poderá conduzir a condenações do Estado Português no TEDH e no pagamento de indemnizações às vítimas por responsabilidade civil no exercício da função jurisdicional.

8. As possibilidades de conservação e utilização de metadados em processos penais em curso após a declaração de inconstitucionalidade dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de julho

Pese embora a declaração de inconstitucionalidade dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008, como acabámos de referir, torna-se imperativo[410] procurar caminhos alternativos no nosso Direito vigente.

Começando pelas normas não declaradas inconstitucionais que permitem obter metadados previamente conservados para o processo são, para quem, como nós, considera que o art. 9.º da Lei n.º 32/2008 foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009[411]:

a) no caso dos dados de base e de localização[412]: art. 14.º, n.º 4, da Lei n.º 109/2009; e

b) no caso dos dados de tráfego: arts. 18.º, n.º 2, da Lei n.º 109/2009[413] (na fase de inquérito) e 189.º, n.º 2, do CPP (nas demais fases processuais)[414].

---

[410] A fim de obstar à violação do princípio da proibição de insuficiência por via do défice de proteção dos direitos fundamentais a que se reconduzem os bens jurídicos tutelados pelos crimes constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 (pese embora consideremos que o art. 9.º da Lei n.º 32/2008 fora revogado pelos arts. 12.º e ss. da Lei n.º 109/2009, aplicando-se aos dados de tráfego o catálogo do art. 18.º, n.º 1, desta Lei e inexistindo catálogo relativamente aos dados de localização e de base) e evitar condenações do Estado português no TEDH (por força dos deveres positivos de levar a cabo investigações criminais relativamente a crimes que lesem direitos fundamentais garantidos pela CEDH que o TEDH tem considerado recaírem sobre as autoridades) e condenações no pagamento de indemnizações às vítimas por responsabilidade civil no exercício da função jurisdicional.

[411] Acerca desta questão, com maiores desenvolvimentos, vide DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 564, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 64 e ss.

[412] RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", in RMP, n.º 172, pp. 50 e ss., considera que o art. 14.º, n.º 4, da Lei n.º 109/2009 não permite a obtenção de dados de localização, na medida em que a al. c) desse n.º 4 (à semelhança do que sucede com o art. 18.º, n.º 3, al. c), da CCiber) exige que tais dados estejam disponíveis com base num contrato ou acordo de serviços; ora, a partir do momento que esses dados estão na posse do fornecedor de serviços em virtude do próprio contrato de prestação de serviços de comunicações eletrónicas, não vemos em que medida o art. 14.º, n.º 4, da Lei n.º 109/2009 não permite a obtenção de dados de localização que estejam na posse do fornecedor de serviços; ademais, o art. 14.º, n.º 4, da Lei n.º 109/2009 permite expressamente a obtenção de dados informáticos que não sejam dados de conteúdo nem dados de tráfego (e os dados de localização, tal como os dados de base, não são uma coisa nem outra).

[413] Na medida em que sempre considerámos que o art. 9.º da Lei n.º 32/2008 revogou parcialmente o art. 189.º, n.º 2, do CPP e que, posteriormente, o art. 9.º da Lei n.º 32/2008 foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009 (apesar do disposto no seu art. 11.º, n.º 2) e tendo em conta que (1) as comunicações a que

Diversamente, para quem entenda que o art. 9.º da Lei n.º 32/2008[415] não foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009:

a) no caso dos dados de base: art. 14.º, n.º 4, da Lei n.º 109/2009; e

b) no caso dos dados de tráfego e de localização, art. 189.º, n.º 2, do CPP[416].

---

se refere o art. 18.º da Lei n.º 109/2009 também geram dados de tráfego e (2) a Lei n.º 109/2009 contém aquilo que podemos denominar como o regime geral da prova digital, o regime relativo à obtenção de dados de tráfego que houvessem sido conservados à luz da Lei n.º 32/2008 terá de constar da Lei n.º 109/2009, como efetivamente consta. De resto, se o art. 9.º da Lei n.º 32/2008 revogou parcialmente o art. 189.º, n.º 2, do CPP, revogado aquele preceito pelos arts. 12.º e ss. da Lei n.º 109/2009 não poderá repristinar-se o art. 189.º, n.º 2, do CPP, apenas restando buscar a norma habilitante da obtenção de dados de tráfego previamente conservados na Lei n.º 109/2009.

Para além disso, o art. 18.º da Lei n.º 109/2009 revogou parcialmente o art. 189.º, n.º 1, do CPP.

Deste modo, também a obtenção, em tempo real, de dados de tráfego gerados no âmbito das comunicações a que se refere o art. 18.º da Lei n.º 109/2009 terá de estar prevista na Lei n.º 109/2009 (pois o art. 187.º do CPP apenas inclui as comunicações por telefone e o art, 189.º, n.º 1, do mesmo Código apenas inclui as conversações entre presentes), como efetivamente consta.

E, por isso, a norma habilitante para a obtenção, em tempo real, de dados de tráfego gerados no âmbito das comunicações a que se refere o art. 18.º da Lei n.º 109/2009 é esse mesmo art. 18.º (pois o art. 14.º exclui os dados de tráfego), por via de uma interpretação hábil do n.º 2 do art. 18.º na parte em que se refere ao "registo de transmissões de dados informáticos". E, igualmente por via de uma interpretação hábil do art 18.º, n.º 2 (e também por igualdade de razão face à obtenção do mesmo tipo de dados em tempo real), a obtenção de dados de tráfego previamente conservados (que restringe direitos fundamentais da mesma forma e na mesma medida que a obtenção em tempo real) também é subsumível ao art. 18.º, n.º 2.

Sem embargo, a fim de afastar quaisquer dúvidas a este respeito, consideramos que a redação do art. 18.º, n.º 2, da Lei n.º 109/2009 deveria ser aperfeiçoada.

(414) Cfr. DUARTE RODRIGUES NUNES/PAULO PINTO DE ALBUQUERQUE, "NOTA PRÉVIA ao Artigo 189.º", in *Comentário do Código de Processo Penal, Vol. I, 5.ª Edição,* p. 860, e DUARTE RODRIGUES NUNES, Curso de Direito Processual Penal, 2, p. 681, e também em "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP,* n.º 170, pp. 48-49.

(415) Que, por sua vez, havia revogado o art. 189.º, n.º 2, do CPP relativamente à obtenção, na fase de inquérito, de dados de tráfego e de localização previamente conservados para a investigação de crimes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 (cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 564-565, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, p. 58).

(416) Cfr. RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", in *RMP,* n.º 172, pp. 74-75, e Acórdãos do STJ de 21/06/2023, da RL de 26/01/2023 e 22/02/2023, da RP de 29/03/2023, da RC de 21/06/2023 e 27/09/2023, da RE de 28/06/2023 e da RG de 02/05/2023.

É certo que o TC – embora de uma forma completamente desproporcionada e desrazoável – considerou que o art. 9.º da Lei n.º 32/2008 é inconstitucional em virtude de não estar prevista a obrigatoriedade da notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros. Todavia, tal poderá ser colmatado por via de, apesar de a Lei não o prever, a autoridade judiciária notificar as pessoas cujos metadados tenham sido acedidos logo que essa notificação não seja suscetível de comprometer as investigações (quer a investigação naquele processo quer noutros processos) nem a vida, a integridade física ou a liberdade (incluindo a liberdade e a autodeterminação sexual) de terceiros[417].

Deste modo, as autoridades podem legitimamente aceder, para fins de investigação criminal, a metadados previamente conservados pelos operadores de comunicações eletrónicas[418].

No entanto, para que esse acesso (e ulterior valoração) possa ter lugar, os metadados terão de ter sido conservados e, mais do que isso, terão de ter sido legitimamente conservados, pelo que, em face da declaração

[417] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP,* n.º 170, p. 49.

[418] Cfr. DUARTE RODRIGUES NUNES/PAULO PINTO DE ALBUQUERQUE, "NOTA PRÉVIA ao Artigo 189.º", in *Comentário do Código de Processo Penal, Vol. I, 5.ª Edição,* p. 860, DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP,* n.º 170, pp. 48-49, RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", in *RMP,* n.º 172, pp. 74-75, e Acórdãos do STJ de 21/06/2023, da RL de 26/01/2023 e 22/02/2023, da RP de 29/03/2023, da RC de 21/06/2023 e 27/09/2023, da RE de 28/06/2023 e da RG de 02/05/2023.

Mesmo antes da entrada em vigor da Lei n.º 109/2009, dado que antes desse momento (e da entrada em vigor da Lei n.º 32/2008) já vigoravam o art. 189.º, n.º 2 (ao abrigo do qual era possível obter dados de tráfego e de localização celular, não distinguindo a Lei se se tratava de dados obtidos em tempo real ou de dados conservados) e os arts. 125.º e 135.º (à luz dos quais era possível obter os dados de base), todos do CPP.

Ademais, antes da entrada em vigor da Lei n.º 32/2008 e da reforma de 2007 do CPP, a jurisprudência admitia a obtenção de dados de tráfego (que eram conservados à luz da Lei n.º 41/2004) junto dos operadores de comunicações eletrónicas (cfr., entre outros, Acórdãos da RC de 17/05/2006 e 15/11/2006, da RG de 10/01/2005 e 21/11/2005 e da RE de 26/06/2007).

de inconstitucionalidade dos arts. 4.º e 6.º da Lei n.º 32/2008, terá(ão) de existir, na nossa ordem jurídica, outra(s) norma(s) que preveja(m) a possibilidade de conservar metadados.

E, de facto, nos termos dos arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004, de 18 de agosto, e 9.º, n.º 2 e 10.º. n.º 1, da Lei n.º 23/96 de 26 de julho (normas que não foram declaradas inconstitucionais pelo TC), os prestadores de serviços de comunicações eletrónicas podem conservar metadados durante 6 meses (que é o período durante o qual a fatura pode ser legalmente contestada e em que o respetivo pagamento pode ser exigido) para fins de faturação dos serviços prestados.

Ainda que a finalidade dessa conservação não seja a utilização probatória dos dados conservados em processos penais, consideramos que, se essa conservação é legalmente admissível para efeitos de salvaguarda de direitos privados de cariz patrimonial dos prestadores de serviços de comunicações eletrónicas (cobrança dos serviços prestados), por maioria de razão, é igualmente legítimo o acesso das autoridades a tais dados (legitimamente conservados) para fins de investigação criminal, prosseguindo-se, dessa forma, o interesse público numa Justiça penal funcionalmente eficaz (que é um pressuposto essencial do Estado de Direito e possui, também ele, respaldo constitucional), sendo que a investigação dos crimes e a punição dos criminosos é levada a cabo em prol do interesse da Comunidade no seu todo e não em prol do engrandecimento do Estado nem de interesses meramente privados[419].

A isto acresce que, como referimos, os arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004, de 18 de agosto, e 9.º, n.º 2 e 10.º. n.º 1, da Lei n.º 23/96 de 26 de julho, não foram declarados inconstitucionais pelo TC.

---

[419] Cfr. DUARTE RODRIGUES NUNES/PAULO PINTO DE ALBUQUERQUE, "NOTA PRÉVIA ao Artigo 189.º", in *Comentário do Código de Processo Penal, Vol. I, 5.ª Edição,* p. 859, DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP,* n.º 170, p. 50, e RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", in *RMP,* n.º 172, p. 72.

And last but not least, é este o entendimento que permite obstar a violações do princípio da proporcionalidade (na vertente de proibição de insuficiência) e evitar condenações do Estado português no TEDH e no pagamento de indemnizações às vítimas, por responsabilidade civil no exercício da função jurisdicional.

Deste modo, consideramos que os metadados conservados pelos prestadores de serviços de comunicações eletrónicas nos termos dos arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004 podem ser utilizados em processos penais[420], assim se obtendo uma concordância prática adequada entre os direitos fundamentais em colisão e obstando aos efeitos nefastos que a impossibilidade de acesso, obtenção e valoração de metadados para fins de investigação criminal poderá ter nos processos em curso (como tem tido) e, sobretudo, nas condenações transitadas em julgado que referimos supra.

E, como também referimos supra, as provas que os metadados podem proporcionar tanto podem servir para provar a prática de crimes pelo arguido como para este demonstrar a sua inocência ou, no mínimo, fazer surgir no julgador uma dúvida razoável.

No entanto, contra este nosso entendimento poderão ser aduzidos vários argumentos, que se nos afiguram totalmente improcedentes.

Assim, em primeiro lugar, poderá aduzir-se que o entendimento que defendemos constitui, na fase de utilização dos metadados, por uma "alienação do fim" *("Zweckentfremdung")*, pois, ao serem subsequentemente acedidos

---

[420] Cfr. DUARTE RODRIGUES NUNES/PAULO PINTO DE ALBUQUERQUE, "NOTA PRÉVIA ao Artigo 189.º", in *Comentário do Código de Processo Penal, Vol. I, 5.ª Edição,* p. 859, DUARTE RODRIGUES NUNES, Curso de Direito Processual Penal, 2, p. 681, e também em "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP*, n.º 170, p. 50, RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", in *RMP,* n.º 172, pp. 61 e ss., e Acórdãos do STJ de 21/06/2023, da RL de 26/01/2023 e 22/02/2023, da RP de 29/03/2023, da RC de 21/06/2023 e 27/09/2023, da RE de 28/06/2023 e da RG de 02/05/2023; contra, Acórdãos da RL de 25/10/2022, da RP de 07/09/2022, 07/12/2022 e 24/05/2023, da RC de 12/10/2022 e da RE de 25/10/2022, 28/02/2023, 09/05/2023 e 12/09/2023.

e valorados num processo penal, os metadados irão ser utilizados para uma finalidade diversa daquela para a qual foram conservados[421]. E, de facto, é isso que acontece.

Contudo, pese embora o que parece resultar do Acórdão do TC n.º 268/2022 (e também do Acórdão *Digital Rights*), o direito à autodeterminação informacional (de que a proibição de "alienação do fim" é um instrumento de tutela) não é absoluto e, além disso, como referimos, a mera conservação de metadados não restringe quaisquer direitos fundamentais (sendo que é a própria Lei n.º 41/2004 que "informa" os utilizadores de comunicações eletrónicas de que os seus metadados podem ser conservados pelos fornecedores de tais serviços) e o ulterior acesso aos mesmos restringe direitos fundamentais de uma forma que não é qualificável como intensa. E, estando em causa a resposta à criminalidade grave, a "alienação do fim" jamais poderá constituir um óbice à obtenção e valoração de metadados para fins de investigação criminal, sob pena de violação da proibição de insuficiência e dos direitos fundamentais a que se reconduzam os bens jurídicos tutelados pelos crimes em causa no caso concreto e que sejam superiores aos direitos à intimidade/privacidade e à autodeterminação informacional[422].

---

[421] Argumento aduzido nos Acórdãos da RP de 07/12/2022 e da RC de 12/10/2022.

Mesmo antes da entrada em vigor da Lei n.º 109/2009, dado que antes desse momento (e da entrada em vigor da Lei n.º 32/2008) já vigoravam o art. 189.º, n.º 2 (ao abrigo do qual era possível obter dados de tráfego e de localização celular, não distinguindo a Lei se se tratava de dados obtidos em tempo real ou de dados conservados) e os arts. 125.º e 135.º (à luz dos quais era possível obter os dados de base), todos do CPP.

Ademais, antes da entrada em vigor da Lei n.º 32/2008 e da reforma de 2007 do CPP, a jurisprudência admitia a obtenção de dados de tráfego (que eram conservados à luz da Lei n.º 41/2004) junto dos operadores de comunicações eletrónicas (cfr., entre outros, Acórdãos da RC de 17/05/2006 e 15/11/2006, da RG de 10/01/2005 e 21/11/2005 e da RE de 26/06/2007).

[422] Cfr. DUARTE RODRIGUES NUNES, "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *RMP,* n.º 170, pp. 50-51, e no essencial (dado que considera que não existe qualquer mudança de finalidade, que, na realidade existe, pois os metadados foram conservados para outra finalidade que não a utilização em processo penal), RUI CARDOSO, "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", in *RMP,* n.º 172, pp. 65-66.

Em segundo lugar, poderá aduzir-se que o TJUE entende que o artigo 15.º, n.º 1, da Diretiva 2002/58/CE (que foi transposta para o Direito português por via da Lei n.º 41/2004), conforme alterada pela Diretiva 2009/136/CE, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da CDFUE, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que preveja, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e de dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica, bem como a uma regulamentação nacional que regule a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União Europeia.

No entanto, os dados conservados nos termos da Lei n.º 41/2004 não se destinam à investigação criminal (como sucedia no caso da Diretiva 2006/24/CE e da Lei n.º 32/2008), pelo que – sem prejuízo das críticas que formulámos supra – a jurisprudência do TJUE não impede a conservação de metadados para as finalidades previstas na Lei n.º 41/2004.

Em terceiro lugar, poderá argumentar-se que aplicar o regime dos arts. 187.º a 189.º do CPP, da Lei n.º 41/2004 e da Lei n.º 109/2009, seria *"deixar entrar pela janela"* aquilo a que o Acórdão do TC n.º 268/2022 *"fechou a porta"*, pois o regime que resultaria da aplicação dos arts. 187.º a 189.º do CPP, da Lei n.º 41/2004 e da Lei n.º 109/2009 padece da mesma falta de garantias que levou à declaração de inconstitucionalidade dos arts. 4.º, 6.º e 9.º da Lei nº 32/2008[423]. No entanto, tendo em conta a crítica que formulámos ao Acórdão do TC n.º 268/2022, *"deixar entrar pela janela"* aquilo que que o TC

[423] Como se faz no Acórdão da RP de 07/12/2022.

terá *"fechado a porta"* mais não será do que evitar violações da própria Constituição e da CEDH (e até da CDFUE), bem como condenações do Estado Português no TEDH e no pagamento de indemnizações às vítimas, por responsabilidade civil no exercício da função jurisdicional.

Esta mesma resposta vale para o argumento de que, "caindo" a Lei n.º 32/2008 e na impossibilidade de aplicação do CPP e da Lei n.º 41/2004, recorrer às normas da Lei n.º 109/2009 seria seguir um caminho espúrio, tendo em conta a declaração de inconstitucionalidade e os fundamentos que a determinaram, não sendo lícito recorrer a "atalhos" como a invocação do disposto no art. 189.º do CPP ou na Lei n.º 109/2009 (para mais quando o art. 11.º, n.º 2, desta Lei determina que o disposto nos arts. 12.º a 19.º dessa Lei não prejudica o regime da Lei n.º 32/2008)[424].

Em quarto lugar, poderia aduzir-se que a aplicação da Lei n.º 109/2009 defraudaria o espírito do legislador, pois o desaparecimento da norma especial (*in casu,* os arts. 3.º e 9.º da Lei n.º 32/2008) não legitima a aplicação da norma geral (*in casu,* as normas da Lei n.º 109/2009)[425]. Contudo, dado que *lex specialis derogat legi generali,* inexistindo ou deixando de existir *lex specialis* (sendo certo que, como resulta do art. 282.º, n.º 1, do CPP, a declaração de inconstitucionalidade com força obrigatória geral produz efeitos *ex tunc* e implica a repristinação das normas revogadas pela norma declarada inconstitucional[426]), haverá que aplicar a *lex generalis,* razão pela qual não existe qualquer fundamento jurídico para negar a aplicabilidade das normas da Lei n.º 109/2009 e do art. 189.º, n.º 2, do CPP[427].

Em quinto lugar, também poderá argumentar-se que os Tribunais não podem substituir-se ao legislador, suprindo omissões de onde resultam graves inconvenientes para a investigação criminal[428]. No entanto, se os

---

[424] Argumento aduzido no Acórdão da RC de 12/10/2022.

[425] Argumento esgrimido nos Acórdãos da RP de 07/12/2022 e da RC de 12/10/2022.

[426] Cfr. GOMES CANOTILHO, Direito Constitucional e Teoria da Constituição, pp. 1000-1001.

[427] Sendo que, para quem entenda que o art. 9.º da Lei n.º 32/2008 não foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009, o art. 189.º, n.º 2, do CPP foi repristinado na parte relativa à obtenção de dados de tráfego e de localização previamente conservados, por via da declaração de inconstitucionalidade com força obrigatória geral do art. 9.º da Lei n.º 32/2008, como prevê o art. 282.º, n.º 1, da CRP.

Sobre o efeito repristinatório da declaração de inconstitucionalidade com força obrigatória geral relativamente às normas revogadas pela norma declarada inconstitucional, vide GOMES CANOTILHO, Direito Constitucional e Teoria da Constituição, pp. 1004-1005.

[428] Cfr. Acórdãos da RP de 07/12/2022 e da RC de 12/10/2022.

demais argumentos são improcedentes, este argumento, mais do que ser também improcedente, é absolutamente inaceitável, pois assenta numa visão completamente ultrapassada dos direitos fundamentais, considerando-os apenas na sua vertente negativa (enquanto *Abwehrrechte*, ou seja, direitos de defesa dos particulares contra os poderes públicos) e ignorando que – à luz da conceção social dos direitos fundamentais, que substituiu a conceção liberal, que os considerava apenas enquanto *Abwehrrechte*) – os direitos fundamentais possuem igualmente uma vertente positiva, prestacional (enquanto *Leistungsrechte*), que obriga o Estado a proteger os direitos fundamentais dos cidadãos também contra ameaças/agressões provenientes de fontes não estatais (*v. g.*, de outros particulares) e da qual resultam os chamados deveres estatais de proteção *(Schutzpflichte)*, cujo incumprimento configura a violação, pelo Estado, de direitos fundamentais e do princípio da proporcionalidade na vertente de proibição de insuficiência[429], que vale também no plano do Direito penal e processual penal[430]. E, como referimos supra, o incumprimento dos deveres estatais de proteção e a violação do princípio da proporcionalidade na vertente de proibição de insuficiência podem resultar, por exemplo, da adoção de medidas inadequadas ou ineficazes, do não aperfeiçoamento das medidas existentes, da adoção de medidas que desprotejam os cidadãos face às ameaças ou agressões provenientes de outros cidadãos ou da "anulação" de medidas existentes de que resulte uma proteção insuficiente de direitos fundamentais[431].

---

[429] Cfr., com maiores desenvolvimentos e amplas referências bibliográficas, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 331 e ss.

[430] Acerca dos corolários do princípio da proporcionalidade na vertente de proibição de insuficiência e dos deveres estatais de proteção ao nível do Direito penal (em sentido amplo), *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 330 e ss., com vastas referências doutrinárias e jurisprudenciais.

[431] Cfr. ISENSEE, Das Grundrecht auf Sicherheit, p. 40, JOSÉ PAULO BALTAZAR JÚNIOR, Crime Organizado e Proibição de Insuficiência, p. 68, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 322, HAIN, "Der Gesetzgeber in der Klemme zwischen Übermass – und Untermassverbot", in *DVBl*, 1993, p. 983, UNRUH, Zur Dogmatik der grundrechtlichen Schutzpflichten, pp. 24-25, e PIETRZAK, "Die Schutzpflicht im verfassungsrechtlichen Kontext – Überblick und neue Aspekte", in JuS, 1994, pp. 750 e 752-753.

Ademais, os deveres estatais de proteção recaem sobre o conjunto das funções do Estado e não apenas sobre a função legislativa, pelo que também os Tribunais e a Administração estão vinculados ao cumprimento desses deveres, porquanto a proteção dos direitos fundamentais não se esgota na aprovação de leis, requerendo também a sua efetiva aplicação[432]; deste modo, o Estado, com a mediação do legislador ordinário ou, em caso de omissão deste, através da atuação dos Tribunais e da Administração, está obrigado a tomar medidas (normativas, judiciais e/ou fácticas) destinadas a proteger os direitos fundamentais contra ameaças/agressões de fontes diversas dos poderes públicos[433].

Este argumento desconsidera, igualmente, a circunstância de, como referimos, a investigação dos crimes e a punição dos criminosos constituírem um meio de proteção de direitos fundamentais e de, por isso, a eficácia da perseguição e da punição de criminosos (que dependem da eficácia da investigação enquanto instrumento de descoberta da verdade material e da obtenção das provas que a sustentam) ser imposta (e não meramente tolerada) pela Constituição e constituir, inclusivamente, um pressuposto essencial do Estado de Direito.

---

[432] Cfr. ISENSEE, Das Grundrecht auf Sicherheit, p. 21, e também em "§ 111.Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht", in *Handbuch des Staatsrechts der Bundesrepublik Deutschland,* V, 2.ª Edição, pp. 146, 147, 190-191 e 218-219, CANARIS, Direitos Fundamentais e Direito Privado, p. 124, GOMES CANOTILHO, "Omissões Normativas e Deveres de Proteção", in Estudos em Homenagem a Cunha Rodrigues, II, p. 119, JORGE REIS NOVAIS, As Restrições aos Direitos Fundamentais Não Expressamente Autorizadas pela Constituição, p. 88, VIEIRA DE ANDRADE, Os Direitos Fundamentais na Constituição Portuguesa de 1976, 3.ª Edição, p. 148, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 317-318 (incluindo a nota 1205), ROBBERS, Sicherheit als Menschenrecht, p. 125, JOSÉ PAULO BALTAZAR JÚNIOR, Crime Organizado e Proibição de Insuficiência, pp. 63 e ss. e 180, e Sentença do BVerfG de 14/05/1985.

[433] Cfr. JORGE REIS NOVAIS, As Restrições aos Direitos Fundamentais Não Expressamente Autorizadas pela Constituição, p. 88, VIEIRA DE ANDRADE, Os Direitos Fundamentais na Constituição Portuguesa de 1976, 3.ª Edição, p. 148, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 317-318 (incluindo a nota 1205), ROBBERS, Sicherheit als Menschenrecht, p. 125, JOSÉ PAULO BALTAZAR JÚNIOR, Crime Organizado e Proibição de Insuficiência, p. 64, Sentença do BVerfG de 16/10/1977, e, em casos-limite, ISENSEE, "§ 111.Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht", in *Handbuch des Staatsrechts der Bundesrepublik Deutschland, V, 2.ª Edição,* pp. 230-231 (alterando a sua opinião anterior); contra, ISENSEE, Das Grundrecht auf Sicherheit, p. 43, UNRUH, Zur Dogmatik der grundrechtlichen Schutzpflichten, p. 24, e DIETLEIN, Die Lehre von den grundrechtlichen Schutzpflichten, 2.ª Edição, p. 72.

Daí que, para mais tendo em conta os efeitos nefastos da decisão do TC e que temos vindo a recensear ao longo deste estudo, os Tribunais não possam demitir-se de procurar caminhos alternativos aos arts, 4.º, 6.º e 9.º da Lei n.º 32/2008 com o argumento (inaceitável) de que compete ao legislador – e não aos Tribunais – solucionar o problema e suprir as omissões de que resultam graves inconvenientes para a investigação criminal, pois, com isso, os Tribunais estarão a demitir-se do seu dever constitucional e legal de proteger os direitos fundamentais dos cidadãos.

Em sexto lugar, também se argumenta[434] que não existe qualquer identidade formal ou material entre o catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 e o catálogo de crimes dos arts. 187.º, n.º 1, e 189.º do CPP e que, por isso, não há que aplicar, por repristinação, nenhuma norma do CPP (o que, de resto, implicaria o desrespeito pela opção do legislador de ter criado um catálogo mais restrito no art. 2.º, n.º 1, al. g), da Lei n.º 32/2008 em vez de considerar como "crimes graves" os crimes constantes do catálogo do n.º 1 do art. 187.º do CPP). Todavia, além de entendermos que o art. 9.º da Lei n.º 32/2008 foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009 (apesar da redação do art. 11.º, n.º 2, desta Lei)[435], a opção do legislador ao criar um catálogo mais restrito no caso do acesso aos metadados conservados do que no caso da obtenção de metadados em tempo real não faz qualquer sentido[436], pelo que não vemos qualquer inconveniente em aplicar a Lei n.º 109/2009 neste tipo de situações. E, quanto à pretensa não repristinação das normas do CPP na sequência da declaração de inconstitucionalidade do art. 9.º da Lei n.º 32/2008, vale o que referimos supra quanto ao argumento de que o desaparecimento da norma especial (*in casu,* os arts. 3.º e 9.º da Lei n.º 32/2008) não legitima a aplicação da

---

[434] Cfr. Acórdão da RC de 12/10/2022.

[435] Relativamente às razões que, na nossa ótica, conduzem a uma tal conclusão, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 563-563, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 65 e ss., com maiores desenvolvimentos e referências bibliográficas.

[436] Pois a obtenção e a valoração de metadados conservados não restringem direitos fundamentais de uma forma mais intensa do que a obtenção desses metadados em tempo real e subsequente valoração.

norma geral (*in casu,* as normas da Lei n.º 109/2009), incluindo no que tange à incompatibilidade deste argumento com o art. 282.º, n.º 1, da CRP.

Em sétimo lugar, aduz-se[437], igualmente, que, tendo em conta os fundamentos da declaração de invalidade da Diretiva 2006/24/CE pelo TJUE, o regime da Lei n.º 32/2008 teria de ser ainda mais restritivo (e daí a declaração de inconstitucionalidade dos arts. 4.º, 6.º e 9.º desta Lei), sendo certo que o regime do art. 189.º, n.º 2, do CPP é menos exigente do que o regime da Lei n.º 32/2008 e que obter ou valorar metadados conservados com base no art. 189.º, n.º 2, do CPP, na Lei n.º 41/2004 e na Lei n.º 109/2009 equivaleria a que a declaração de inconstitucionalidade produzisse o efeito contrário àquele que pretendeu (pois permitiria a aplicação de um regime menos restritivo do que o regime dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008).

Relativamente a estes argumentos, tendo em conta tudo o que temos vindo a referir (incluindo o que referimos quanto à jurisprudência do TJUE em matéria de metadados e ao Acórdão do TC n.º 268/2022), o facto de o regime que resulta da aplicação do art. 189.º, n.º 2, do CPP, da Lei n.º 41/2004 e da Lei n.º 109/2009 ser – e é, e bem – menos restritivo do que o regime do art. 9.º da Lei n.º 32/2008 não é minimamente impeditivo da obtenção e valoração probatória, em processos penais, de metadados conservados pelos prestadores de serviços de comunicações eletrónicas nos termos dos arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004.

Por isso, reiteramos que, apesar do decidido pelo TC no seu Acórdão n.º 268/2022, são lícitas, à luz da legislação vigente, a obtenção e valoração probatória, em processos penais, de metadados conservados pelos prestadores de serviços de comunicações eletrónicas nos termos dos arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004, assim como, na nossa ótica, o entendimento contrário, além de não ter apoio na Lei, viola a CRP, a CEDH e mesmo a própria CEDFUE.

[437] Cfr. Acórdão da RC de 12/10/2022.

9. As alterações à Lei n.º 32/2008 aprovadas pela Assembleia da República. A nossa apreciação

Ciente da absoluta necessidade da conservação e da utilização probatória de metadados conservados na investigação criminal, o legislador, apesar da estreitíssima (ou mesmo inexistente) margem de manobra que lhe foi deixada pelo Acórdão do TC n.º 268/2022 e pela própria jurisprudência do TJUE[438] posterior ao Acórdão *Digital Rights*, procurou elaborar nova legislação – introduzindo modificações na Lei n.º 32/2008 – relativa à conservação e à utilização probatória de metadados conservados na investigação criminal.

Tendo sido apresentados uma Proposta de Lei pelo Governo e Projetos de Lei pelo PSD, CH e PCP relativos à alteração da Lei n.º 32/2008 após o Acórdão do TC n.º 268/2002 e sido constituído um Grupo de Trabalho na Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República (no âmbito do qual fomos ouvidos, por indicação da IL), foi aprovado, em 13 de outubro de 2023, o Texto de substituição e relatório de nova apreciação na generalidade da Proposta de Lei n.º 11/XV/1.ª (GOV), e Projetos de Lei n.os 70/XV/1.ª (PSD), 79/XV/1.ª (CH) e 100/XV/1.ª (PCP). Tendo o diploma aprovado sido enviado para promulgação, o Presidente da República remeteu-o ao TC para fiscalização preventiva da sua constitucionalidade, o que se justifica plenamente.

O diploma aprovado, que reproduz a redação da Proposta de Lei n.º 11/XV/1.ª (GOV) e do Projeto de Lei n.º 70/XV/1.ª (PSD)[439], é, na nossa opinião, merecedor de elogio, mas também de algumas observações e críticas,

---

[438] Que, atenta a situação de Portugal, no que tange à luta contra a criminalidade grave, apenas permitem a conservação generalizada e indiferenciada de endereços IP atribuídos à fonte de uma ligação e de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos, uma vez que a conservação seletiva dos dados de tráfego e dos dados de localização nos termos propostos pelo TJUE é absolutamente inviável, como demonstrámos supra.

[439] Disponível em https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063484d364c793968636d356c6443397a6158526c63793959566b786c5a793944543030764d554e425130524d5279394562324e316257567564473975a5357357059326c6864476c3259554e7662576c7a633246764c325a685a5442694d5749794c546b354f4755744e4468694e4330344d7a59304c5442685a4451344d57466c596a4d325a5335775a47593d&fich=fae0b1b2-998e-48b4-8364-0ad481aeb36e.pdf&Inline=true.

salientando-se, desde já, a coragem do legislador ao insistir – pese embora a estreitíssima (ou mesmo inexistente) margem de manobra que lhe foi deixada pelo Acórdão do TC n.º 268/2022 e pela própria jurisprudência do TJUE posterior ao Acórdão *Digital Rights* – na previsão da conservação "preventiva" de metadados (incluindo no caso dos dados de tráfego e de localização) para efeitos de investigação criminal.

Vejamos, com maior pormenor, os aspetos mais relevantes das alterações introduzida pelo diploma aprovado à Lei n.º 32/2008.

9.1 Artigo 4.º da Lei n.º 32/2008

Concordamos com a exigência de que a conservação dos dados tenha lugar em Portugal ou no território de outro Estado-Membro da União Europeia, pois, desse modo, são cumpridas, sem qualquer margem para dúvidas, as exigências do TC e do TJUE e sem que daí resulte qualquer prejuízo para a investigação da criminalidade (*maxime* da criminalidade grave).

Ao ser mantido, quanto ao mais, o disposto no art. 4.º da Lei n.º 32/2008 entretanto julgado inconstitucional (seja a conservação "preventiva" sejam as tipologias de metadados a conservar) – aplaudindo-se a coragem do legislador neste ponto e a sua consciência quanto à absoluta necessidade deste instrumento para responder eficazmente à criminalidade –, não está a ser observada nem a jurisprudência do TC nem a jurisprudência do TJUE, visto que se trata de uma conservação generalizada e indiferenciada.

Todavia, tendo em conta o que viemos referindo quanto ao Acórdão do TC n.º 268/2022 e à jurisprudência do TJUE em matéria de conservação e utilização probatória de metadados, o legislador português só observará o disposto na CRP, na CEDH e mesmo na CDFUE se previr a conservação "preventiva" de metadados nos termos que já previa e volta a prever no art. 4.º da Lei n.º 32/2008, esperando-se que o TC repondere o entendimento desrazoável e inconstitucional que perfilhou no Acórdão n.º 268/2022.

Aliás, se dúvidas ainda existirem acerca da desrazoabilidade do entendimento do TJUE, que o TC acolheu, basta ver que, por exemplo, o legislador alemão, malgrado as várias tentativas que já levou a cabo nesse sentido, não consegue elaborar uma lei em matéria de conservação de metadados que o TJUE considere que observa o seu entendimento.

E a isto acresce que, se, por hipótese, na sequência do conflito entre o Estado de Israel e a organização terrorista Hamas, organizações terroristas islâmicas decidissem "acordar" os seus membros "adormecidos" que se encontrem em Estados-Membros da União Europeia, a continuar a vingar a jurisprudência do TJUE acolhida pelo TC e por um setor da jurisprudência dos Tribunais comuns, na maioria desses países, as autoridades não poderiam obter nem valorar dados de tráfego ou dados de localização que tivessem sido alvo de conservação e, após a ocorrência dos atentados, os dados de tráfego e/ou de localização obtidos em tempo real dificilmente teriam alguma utilidade para a investigação desses atentados.

Deste modo, ainda que existam caminhos alternativos no Direito vigente em matéria de conservação dos metadados e da sua utilização probatória em processos penais, é preferível voltar a prever expressamente essa possibilidade num diploma relativo ao combate à criminalidade, pois permite evitar quaisquer dúvidas, sobretudo quando continuam a ser proferidas decisões pelos Tribunais comuns que não autorizam a obtenção e utilização de metadados em processos penais e anulam as provas obtidas por via dos metadados conservados, rejeitando os caminhos alternativos que existem na Lei vigente.

9.2 Artigo 6.º da Lei n.º 32/2008

Relativamente ao n.º 1 do art. 6.º da Lei n.º 32/2008, na medida em que se entende maioritariamente que o IP é um dado de base[440], talvez se justificasse inverter a ordem das als. b) e c), passando a constar da al. b)

---

[440] Sobre a subsunção do IP (estático e dinâmico) à categoria dos dados de base ou à categoria dos dados de tráfego, vide DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 227 (nota 861), e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, 2.ª Edição, pp. 110-111, com referências doutrinais e jurisprudenciais.

os "endereços de protocolo IP atribuídos à fonte de uma ligação" e da al. c) os "demais dados de base".

Passando ao n.º 2 do art. 6.º, existe uma incongruência face aos arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004, de 18 de agosto, e 9.º, n.º 2 e 10.º. n.º 1, da Lei n.º 23/96 de 26 de julho, pois, se os operadores de comunicações eletrónicas podem conservar os metadados por 6 meses para cobrança dos serviços prestados, por maioria de razão, no caso da conservação para fins de resposta à criminalidade grave, o prazo de conservação deveria ser, pelo menos, o mesmo[441].

Também não faz sentido presumir o consentimento no sentido da prorrogação do prazo de conservação para 6 meses até porque, no nosso Direito, no consentimento presumido, estão em causa situações de perigo na demora e de impossibilidade de obter o consentimento expresso em tempo útil, sendo que, no caso da conservação de metadados, não se verifica qualquer situação dessa natureza[442]. Além disso, para que o consentimento possa ser presumido, é necessário que seja razoável supor que, em face das circunstâncias do caso concreto, o visado teria prestado consentimento se tivesse sido consultado, não nos parecendo que seja possível formular uma tal suposição no que concerne à extensão do prazo de conservação de dados de tráfego e de dados de localização, sobretudo quando esses dados podem ser utilizados como prova contra o respetivo titular.

Quanto aos n.os 3 e 6, não nos parece que exista qualquer justificação para a atribuição da competência a um coletivo de Juízes do STJ: se um Tribunal de Comarca pode condenar em penas de 25 anos de prisão e um Juiz de 1.ª Instância pode determinar a prisão preventiva ou autorizar o recurso a meios de obtenção de prova muito mais restritivos de direitos do que a conservação de metadados (que nem sequer restringe direitos fundamentais), inexiste qualquer razão para que tenha de intervir um coletivo de Juízes do STJ.

---

[441] Sem prejuízo de entendermos que o prazo de 1 ano, também no caso dos dados de tráfego e de localização, era razoável e não violava a Constituição.

[442] Sobre o consentimento presumido, vide DUARTE RODRIGUES NUNES, Curso de Direito Penal, Parte Geral, Tomo I, 2.ª Edição, pp. 460 e ss.

De todo o modo, parecendo que a prorrogação prevista no n.º 3 dependerá da ocorrência de circunstâncias excecionais (como parece resultar do n.º 4), ao ponto de justificarem a intervenção do PGR, nesse caso, fará sentido que a prorrogação seja decidida pelo STJ, embora nos pareça excessiva a intervenção de um coletivo, sobretudo quando a mera conservação não restringe quaisquer direitos fundamentais.

Por fim, quanto ao n.º 5 do art. 6.º, existe o risco de este preceito vir a ser interpretado no sentido de constituir mais um argumento contra a admissibilidade da utilização probatória dos metadados armazenados nos termos da Lei n.º 41/2004, caso o TC, ao não reponderar o seu entendimento, volte a considerar que o art. 4.º e o art. 9.º da Lei n.º 32/2008 são inconstitucionais[443].

9.3 Artigo 7.º da Lei n.º 32/2008

As alterações introduzidas parecem-nos adequadas, existindo uma salutar preocupação em incrementar as garantias de inviolabilidade dos dados conservados.

9.4 Artigo 9.º da Lei n.º 32/2008

Pese embora sempre tenhamos entendido que, apesar do disposto no art. 11.º, n.º 2, da Lei n.º 109/2009, o art. 9.º da Lei n.º 32/2008 foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009, entendemos que teria sido preferível introduzir melhoramentos na Lei n.º 109/2009 (por exemplo, introduzir o que consta dos n.os 7 a 9 do art. 9.º da Lei n.º 32/2008 nos arts. 14.º e 18.º da Lei n.º 109/2009, revogar o n.º 2 do art. 11.º da Lei n.º 109/2009, e clarificar a subsunção da obtenção dos dados de tráfego ao art. 18.º, n.º 2) em vez de reformular o art. 9.º da Lei n.º 32/2008.

---

[443] Por isso, apesar de termos inicialmente entendido que tal clarificação da lei se justificaria (como consta do documento que elaborámos para apoio à nossa audição Grupo de Trabalho dos Metadados da 1.ª Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República e que cedemos a esse Grupo de Trabalho), temos agora sérias reservas acerca da bondade do disposto no n.º 5 do art. 6.º da Lei n.º 32/2008.

De todo o modo, tendo o legislador optado por reformular o art. 9.º da Lei n.º 32/2008, nos termos em que o fez, concordamos com o aditamento daquilo que consta dos n.os 7 a 9 (a fim de observar a jurisprudência do TJUE e do TC); contudo, também entendemos que deveria ter sido estabelecida uma exceção relativa aos casos em que a notificação dos titulares dos metadados que tenham sido acedidos possa prejudicar outras investigações em curso e não apenas a investigação em que os metadados foram utilizados.

No que tange ao n.º 2 do art. 9.º da Lei n.º 32/2008, tendo em conta o critério previsto nos arts. 268.º, n.º 2, e 269.º, n.º 2, do CPP[444], deveria prever-se, também aqui, a possibilidade de, em casos de perigo na demora, o pedido de acesso ser apresentado ao Juiz diretamente pela autoridade de polícia criminal ou mesmo a possibilidade de a autorização ser concedida pelo MP, embora com sujeição a ulterior ratificação expressa do Juiz (o que, na nossa ótica, não contradiz a jurisprudência do TJUE, pois existe uma intervenção, ainda que a *posteriori,* do Juiz).

O que consta dos demais números do art. 9.º da Lei n.º 32/2008 merece a nossa concordância, sem prejuízo de entendermos que o catálogo de crimes constante do art. 2.º, n.º 1, al. g), dessa Lei é excessivamente restritivo e que não se justifica a existência, na nossa ordem jurídica, de dois regimes diversos de obtenção de dados de localização e de dados de base, consoante a mesma ocorra em tempo real (a que se aplicará o regime do art. 14.º da Lei n.º 109/2009, que não contém qualquer elenco de crimes ou de alvos nem exige autorização judicial prévia na fase de inquérito) ou incida sobre dados conservados (a que se aplicaria o art. 9.º da Lei n.º 32/2008), porquanto o facto de os dados terem sido conservados não aumenta a lesividade da sua transmissão; e o mesmo vale quanto aos dados de tráfego, em que, se a obtenção ocorrer em tempo real, aplicar-se-á, consoante o entendimento, o art. 18.º da Lei n.º 109/2009 ou o art. 189.º, n.º 2, do CPP (cujos catálogos de crimes são muito mais amplos do que o do art. 2.º, n.º 1, al. g), da Lei n.º 109/2009), ao passo que, se incidir sobre dados conservados, aplicar-se-á o art. 9.º da Lei n.º 32/2008.

---

(444) Em que se prevê a possibilidade de a autoridade de polícia criminal, em caso de urgência ou de perigo na demora, poder requerer diretamente ao JIC a prática de atos que devem ser praticados pelo JIC ou a autorização para a prática de atos que têm de ser autorizados pelo JIC.

9.5 Artigos 16.º e 17.º da Lei n.º 32/2008

As alterações introduzidas afiguram-se-nos adequadas ao poderem proporcionar a deteção de situações menos corretas e a sua correção, quer para incrementar a eficácia da conservação e da utilização probatória de metadados quer para impedir restrições desnecessárias e/ou desproporcionadas dos direitos fundamentais dos titulares dos metadados.

10 Conclusões

a) A Lei n.º 32/2008, de 17 de junho transpôs para a nossa ordem jurídica a Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações (metadados);

b) A conservação e a transmissão dos metadados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes, sendo obrigatória a separação dos ficheiros destinados à conservação de dados de quaisquer outros ficheiros para outros fins.

c) As provas que os metadados podem proporcionar tanto podem servir para provar a prática de crimes pelo arguido como para este demonstrar a sua inocência ou, no mínimo, fazer surgir no julgador uma dúvida razoável

d) Nos termos do art. 9.º da Lei n.º 32/2008, os metadados só podiam ser desbloqueados (*i.e.,* desencriptados) para efeitos de transmissão às autoridades competentes, que, nos termos do art. 2.º, n.º 1, al. f), são as autoridades judiciárias (Juiz, JIC e MP) e as autoridades de polícia criminal e, desde que se tratasse de metadados relativos ao arguido, ao suspeito, ao intermediário ou à vítima (neste último caso, mediante o respetivo consentimento);

e) O art. 9.º da Lei n.º 32/2008 fora já tacitamente revogado pelos arts. 12.º e ss. da Lei n.º 109/2009, de 15 de setembro;

f) Na sequência de o TJUE, em 2014, ter declarado a Diretiva 2006/24/CE inválida e apesar das garantias previstas na Lei n.º 32/2008 (que não padecia dos vícios que haviam levado o TJUE a declarar a invalidade da Diretiva), o TC, embora com um voto de vencido, declarou a inconstitucionalidade, com força obrigatória geral, dos arts. 4.º, 6.º e 9.º da Lei n.º 32/2008;

g) O TJUE (no Acórdão *Digital Rights*) e o TC não realizaram qualquer ponderação entre os interesses em conflito, tendo desconsiderado, em absoluto, os direitos fundamentais (garantidos pela CDFUE e pela CRP) prosseguidos através da investigação criminal;

h) Na sua jurisprudência relativa à conservação e à utilização probatória de metadados subsequente ao Acórdão *Digital Rights*, o TJUE passou a fundamentar as decisões com base numa ponderação de interesses, embora formulando exigências (1) impossíveis de cumprir, (2) desconformes com a realidade da criminalidade da atualidade, (3) de difícil (ou mesmo impossível) determinação e (4) que abrem a porta a um tratamento discriminatório entre os cidadãos;

i) A jurisprudência do TJUE relativa à conservação e utilização probatória de metadados viola a CEDH, a CRP e a própria CEDFUE;

j) O TC não estava obrigado a seguir a jurisprudência do TJUE no Acórdão *Digital Rights* (e, ao acolhê-la violou o disposto nos arts. 8.º, n.º 4, *in fine,* da CRP e 53.º da CDFUE), sendo que o Acórdão n.º 268/2022 padece de problemas ainda mais graves do que o Acórdão *Digital Rights*;

k) O entendimento plasmado no Acórdão do TC n.º 268/2022 (1) é desconforme com a realidade da criminalidade atual e da investigação dessa mesma criminalidade (cujas necessidades ignora em absoluto), (2) considera que mera conservação de metadados restringe direitos fundamentais, quando, na realidade, não restringe qualquer direito fundamental, (3) considera que a conservação generalizada e indiferenciada e a obtenção de dados de tráfego e de localização restringem direitos fundamentais de forma intensa, quando, na realidade, a obtenção de tais dados, ainda que restrinja direitos fundamentais, não o faz de uma forma intensa, (4) desconsidera, em absoluto, os direitos fundamentais a que se reconduzem os bens jurídicos tutelados pelos crimes

constantes do catálogo do art. 2.º, n.º 1, al. g), da Lei n.º 32/2008, (5) considera inconstitucional a conservação de metadados para fins de investigação criminal de crimes graves, apesar de os prestadores de serviços de comunicações eletrónicas poderem conservar metadados durante 6 meses para fins de faturação dos serviços prestados, (6) é passível de comprometer seriamente a investigação de muitos crimes, (7) viola a CEDH, podendo conduzir a condenações do Estado Português no TEDH e, na sequência dessas condenações, à condenação no pagamento de indemnizações às vítimas por responsabilidade civil no exercício da função jurisdicional, (8) viola o disposto nos arts. 8.º, n.º 4, in fine, da CRP e 53.º da CDFUE, (9) viola o princípio da presunção de inocência, (10) viola o princípio da não discriminação no tratamento de dados pessoais, (11) viola o princípio do processo equitativo, (12) viola o princípio da proporcionalidade na vertente de proibição de insuficiência e (13) pode conduzir a condenações e a absolvições materialmente injustas (em virtude da impossibilidade de obtenção e de valoração de metadados) e à revogação de condenações transitadas em julgado; l) A Lei vigente permite evitar as consequências nefastas referidas na conclusão anterior, dado que o art. 14.º, n.º 4, da Lei n.º 109/2009 (no caso dos dados de base e de localização) e, no caso dos dados de tráfego, os arts. 18.º, n.º 2, da Lei n.º 109/2009 (na fase de inquérito) e 189.º, n.º 2, do CPP (nas demais fases processuais) permitem obter dados de base, bem como os dados de tráfego e/ou de localização que tenham sido conservados pelos operadores de comunicações eletrónicas ao abrigo dos arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004, ainda que essa conservação se destinasse à cobrança dos serviços prestados aos clientes;

m) O legislador aprovou já um diploma que introduz diversas alterações à Lei n.º 32/2008, em que tenta reformular o regime da conservação e da utilização probatória, em processos penais, de metadados conservados após a declaração de inconstitucionalidade, com força obrigatória geral, os arts. 4.º, 6.º e 9.º da Lei n.º 32/2008, sendo essas alterações merecedoras da nossa concordância em alguns aspetos e da nossa crítica noutros.

Bibliografia

Andrade, José Carlos Vieira de – Os Direitos Fundamentais na Constituição Portuguesa de 1976, 3.ª Edição, Almedina, Coimbra, 2004.

Canaris, Claus-Wilhelm – Direitos Fundamentais e Direito Privado (traduzido por Ingo Wolfgang Sarlet e Paulo Mota Pinto), 2.ª Reimpressão, Almedina, Coimbra, 2009.

Canotilho, José Joaquim Gomes – "Omissões Normativas e Deveres de Protecção", in *Estudos em Homenagem a Cunha Rodrigues,* Volume II, pp. 111 e ss, Coimbra Editora, Coimbra, 2001.

Canotilho, José Joaquim Gomes – Direito Constitucional e Teoria da Constituição, 5.ª Edição, Almedina, Coimbra, 2002.

Canotilho, José Joaquim Gomes/Moreira, Vital – Constituição da República Portuguesa Anotada, Volume I, 4.ª Edição, Coimbra Editora, Coimbra, 2007.

Cardoso, Rui – "A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", in Revista do Ministério Público, n.º 172, pp. 9 e ss., Lisboa, 2022.

Correia, João Conde – "Prova digital: as leis que temos e a lei que devíamos ter", in Revista do Ministério Público, n.º 139, pp. 29 e ss., Lisboa, 2014.

Dias, Jorge de Figueiredo – Acordos Sobre a Sentença em Processo Penal, O "Fim" do Estado de Direito ou um Novo "Princípio"?, Conselho Distrital do Porto da Ordem dos Advogados, Porto, 2011.

Dias, Jorge de Figueiredo – Direito Penal, Parte Geral, Tomo I, Questões fundamentais, A doutrina geral do crime, 3.ª Edição, Coimbra Editora, Coimbra, 2019.

Dietlein, Johannes – Die Lehre von den grundrechtlichen Schutzpflichten, 2.ª Edição, Duncker&Humblot, Berlim, 2005.

Hain, Karl-Eberhard – "Der Gesetzgeber in der Klemme zwischen Übermass – und Untermassverbot", in *Deutsches Verwaltungsblatt*, Ano 108, Fascículo 18, pp. 982 e ss., Carl Heymanns Verlag, Colónia, Berlim, Bona, Munique, 1993.

Isensee, Josef – Das Grundrecht auf Sicherheit, Zu den Schutzpflichten des freiheitlichen Verfassungsstaates, Walter de Gruyter, Berlim e Nova Iorque, 1983.

Isensee, Josef – "§ 111.Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht", in *Handbuch des Staatsrechts der Bundesrepublik Deutschland,* Volume V, Allgemeine Grundrechtslehren, 2.ª Edição, pp. 143 e ss., C.F.Müller Juristischer Verlag, Heidelberg, 2000.

Júnior, José Paulo Baltazar – Crime Organizado e Proibição de Insuficiência, Livraria do Advogado, Porto Alegre, 2010.

Novais, Jorge Reis – As Restrições aos Direitos Fundamentais Não Expressamente Autorizadas pela Constituição, Coimbra Editora, Coimbra, 2003.

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

Nunes, Duarte Rodrigues – "Da admissibilidade da obtenção de dados de localização celular ou de dados de tráfego de todos os telemóveis/cartões que acionaram um determinado conjunto de antenas/células de telecomunicações no lapso de tempo em que o crime sob investigação terá sido praticado, para posterior identificação dos seus autores.", in *Revista do Ministério Público,* n.º 157, pp. 125 e ss., Lisboa, 2019.

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

Nunes, Duarte Rodrigues – "Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor?", in *Revista do Ministério Público* n.º 170, pp. 9 e ss., Sindicato dos Magistrados do Ministério Público, Lisboa, 2022.

Nunes, Duarte Rodrigues – Curso de Direito Penal, Parte Geral, Tomo I, Questões fundamentais, Teoria geral do crime, 2.ª Edição, Gestlegal, Coimbra, 2023.

Nunes, Duarte Rodrigues – Curso de Direito Processual Penal, 1, Noções gerais, Elementos do processo penal, Universidade Católica Editora, Lisboa, 2023.

Nunes, Duarte Rodrigues – Curso de Direito Processual Penal, 2, Elementos do processo penal (continuação), O procedimento criminal, Universidade Católica Editora, Lisboa, 2023.

Nunes, Duarte Rodrigues/Albuquerque, Paulo Pinto de – "Artigo 172.º", in *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem,* Vol. I, 5.ª Edição, pp. 721 e ss., Universidade Católica Editora, Lisboa, 2023.

Nunes, Duarte Rodrigues/Albuquerque, Paulo Pinto de – "NOTA PRÉVIA ao Artigo 189.º", in *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem,* Vol. I, 5.ª Edição, pp. 856 e ss., Universidade Católica Editora, Lisboa, 2023.

Pietrzak, Alexandra – "Die Schutzpflicht im verfassungsrechtlichen Kontext – Überblick und neue Aspekte", in *Juristische Schulung, 1994,* pp. 748 e ss., Verlag C. H. Beck, Munique e Frankfurt, 1994.

Robbers, Gerhard – Sicherheit als Menschenrecht, Aspekte der Geschichte, Begründung unsd Wirkung einer Grundrechtsfunktion, Nomos Verlag, Baden-Baden, 1987.

Unruh, Peter – Zur Dogmatik der grundrechtlichen Schutzpflichten, Duncker&Humblot, Berlim, 1996.

Jurisprudência

Tribunal Europeu dos Direitos Humanos

Acórdão McCann e Outros c. Reino Unido (de 27 de setembro de 1995),
In *https://hudoc.echr.coe.int/.*

Acórdão Mahmut Kaya c. Turquia (de 28 de março de 2000),
in *https://hudoc.echr.coe.int/.*

Acórdão Hugh Jordan c. Reino Unido (de 4 de maio de 2001),
in *https://hudoc.echr.coe.int/.*

Acórdão Paul e Audrey Edwards c. Reino Unido (de 14 de março de 2002),
in *https://hudoc.echr.coe.int/.*

Acórdão Nachova e Outros c. Bulgária *(de 6 de julho de 2005),*
in *https://hudoc.echr.coe.int/.*

Acórdão Kaya e Outros c. Turquia (de 24 de outubro de 2006),
in *https://hudoc.echr.coe.int/*.

Acórdão Ramsahai e Outros c. Países Baixos (de 15 de maio de 2007),
in *https://hudoc.echr.coe.int/.*

Acórdão Angelova e Iliev c. Bulgária (de 26 de julho de 2007),
in *https://hudoc.echr.coe.int/.*

Acórdão K.U. c. Finlândia (de 2 de dezembro de 2008),
in *https://hudoc.echr.coe.int/.*

Acórdão Opuz c. Turquia (de 9 de junho de 2009),
in *https://hudoc.echr.coe.int/.*

Acórdão Kolevi c. Bulgária (de 5 de novembro de 2009),
in *https://hudoc.echr.coe.int/.*

Acórdão Al-Skeini e Outros c. Reino Unido (de 7 de julho de 2011),
in *https://hudoc.echr.coe.int/.*

Acórdão Vasîlka c. Moldávia (de 11 de fevereiro de 2014),
in *https://hudoc.echr.coe.int/.*

Acórdão Jaloud c. Países Baixos (de 20 de novembro de 2014),
in *https://hudoc.echr.coe.int/.*

Acórdão Mustafa Tunç e Fecire Tunç c. Turquia (de 14 de abril de 2015),
in *https://hudoc.echr.coe.int/.*

Acórdão Armani da Silva c. Reino Unido (de 30 de março de 2016),
in *https://hudoc.echr.coe.int/.*

Acórdão Khadija Ismayilova c. Azerbaijão (de 10 de janeiro de 2019),
in *https://hudoc.echr.coe.int/.*

Acórdão Big Brother Watch e Outros c. Reino Unido (de 25 de maio de 2021),
in *https://hudoc.echr.coe.int/.*

Acórdão Volodina c. Rússia (n.º 2) (de 14 de setembro de 2021),
in *https://hudoc.echr.coe.int/.*

Tribunal de Justiça da União Europeia

Acórdão *Digital Rights* Ireland Ltd e Kärntner Landesregierung e Outros
(de 8 de abril de 2014, Processos C-293/12 e C-594/12),
in *http://curia.europa.eu.*

Acórdão Tele2 Sverige AB e Secretary of State for the Home Department
(de 21 de dezembro de 2016, Processos C-203/15 e C-698/15),
in *http://curia.europa.eu.*

Acórdão Ministerio Fiscal (de 2 de outubro de 2018, Processo C-207/16),
in *http://curia.europa.eu.*

Acórdão Privacy International (de 6 de outubro de 2020, Processo C-623/17),
in *http://curia.europa.eu.*

Acórdão La Quadrature du Net e Outros
(de 6 de outubro de 2020, Processos C-511/18, C-512/18 e C-520/18),
in *http://curia.europa.eu.*

Acórdão Prokuratuur (de 2 de março de 2021, Processo C-746/18),
in *http://curia.europa.eu*

Acórdão G. D. e Commissioner of An Garda Síochána
(de 5 de abril de 2022, Processo C-140/20),
in *http://curia.europa.eu.*

Acórdão SpaceNet e Telekom Deutschland
(de 20 de setembro de 2022, Processos C-793/19 e C-794/19),
in *http://curia.europa.eu.*

Acórdão A. G. e Lietuvos Respublikos generalinė prokuratūra
(de 7 de setembro de 2023, Processo *C-162/22),*
in http://curia.europa.eu.

Portugal
Tribunal Constitucional

Acórdão n.º 213/2008, in *www.tribunalconstitucional.pt.*
Acórdão n.º 403/2015, in *www.tribunalconstitucional.pt.*
Acórdão n.º 464/2019, in *www.tribunalconstitucional.pt.*
Acórdão n.º 268/2022, in *www.tribunalconstitucional.pt.*

Tribunal Constitucional

Acórdão de 3 de março de 2010 (Processo 886/07.8PSLSB.L1.S1), in *www.dgsi.pt.*
Acórdão de 29 de abril de 2010 (Processo 128/05.0JDLSB-A.S1), in *www.dgsi.pt.*
Acórdão de 21 de setembro de 2022 (Processo 79/13.5JBLSB-C.S1), in *www.dgsi.pt.*
Acórdão de 10 de novembro de 2022 (Processo 120/17.2TELSB-B.S1), in *www.dgsi.pt.*
Acórdão de 19 de janeiro de 2023 (Processo 33/15.2JAPRT-B.S1), in *www.dgsi.pt.*
Acórdão de 1 de fevereiro de 2023 (Processo 35/17.4GACHV-A.S1), in *www.dgsi.pt.*
Acórdão de 11 de maio de 2023 (Processo 21/11.8PEPRT-M.S1), in *www.dgsi.pt.*
Acórdão de 21 de junho de 2023 (Processo 1229/19.3TELSB-A.S1), in *www.dgsi.pt.*
Acórdão de 29 de junho de 2023 (Processo 42/10.8PBVCD-B.S1), in *www.dgsi.pt.*

Tribunal da Relação de Coimbra

Acórdão de 17 de maio de 2006 (Processo 1265/06), in *www.dgsi.pt.*
Acórdão de 15 de novembro de 2006 (Processo 915/06.2TAAVR-A.C1), in *www.dgsi.pt.*
Acórdão de 12 de outubro de 2022 (Processo 538/22.9JALRA.C1), in *www.dgsi.pt.*
Acórdão de 21 de junho de 2023 (Processo 302/21.2JACBR.C1), inédito.
Acórdão de 27 de setembro de 2023 (Processo 13/20.6PEVIS.C1), in *www.dgsi.pt.*

Tribunal da Relação de Évora

Acórdão de 26 de junho de 2007 (Processo 843/07-1), in *www.dgsi.pt.*
Acórdão de 25 de outubro de 2022 (Processo 52/18.7GBSLV.E1), in *www.dgsi.pt.*
Acórdão de 28 de fevereiro de 2023 (Processo 661/17.1TELSB.E1), in *www.dgsi.pt.*
Acórdão de 9 de maio de 2023 (Processo 275/22.4GCSTB-A.E1), in *www.dgsi.pt.*
Acórdão de 28 de junho de 2023 (Processo 2010/21.5JFLSB-A.E1), in *www.dgsi.pt.*
Acórdão de 12 de setembro de 2023 (Processo 950/10.6PCSTB.E2), in *www.dgsi.pt.*

Tribunal da Relação de Guimarães

Acórdão de 10 de janeiro de 2005 (Processo 2013/04-1), in *www.dgsi.pt.*
Acórdão de 21 de novembro de 2005 (Processo 1987/05-1), in *www.dgsi.pt.*
Acórdão de 2 de maio de 2023 (Processo 12/23.6 PBGMR-A.G1), in *www.dgsi.pt.*

Tribunal da Relação de Lisboa

Acórdão de 24 de janeiro de 2012 (Processo 35/07.2PJAMD.L1-5), in *www.dgsi.pt.*
Acórdão de 25 de outubro de 2022 (Processo 50/22.6JBLSB-A.L1-5), in *www.dgsi.pt.*
Acórdão de 26 de janeiro de 2023 (Processo 849/20.8PBCSC.L1-9), in *www.dgsi.pt.*
Acórdão de 22 de fevereiro de 2023 (Processo 495/22.1JAFUN-A.L1-5), in *www.dgsi.pt.*

Tribunal da Relação do Porto

Acórdão de 7 de dezembro de 2022 (Processo 5011/22.2JAPRT-A.P1), in *www.dgsi.pt.*
Acórdão de 29 de março de 2023 (Processo 47/22.6PEPRT-Z.P1), in *www.dgsi.pt.*
Acórdão de 24 de maio de 2023 (Processo 747/20.5JGLSB.P1), in *www.dgsi.pt.*

Alemanha

Bundesverfassungsgericht

Sentença de 16 de outubro de 1977 (1 BvQ 5/77), in *https://www.bundesverfassungsgericht.de.*

Sentença de 14 de maio de 1985 (1 BvR 233/81; 1 BvR 341/81),
in *https://www.servat.unibe.ch/dfr/bv069315.html (consultado em 30/10/2023).*

Sentença de 2 de março de 2010 (1 BvR 256/08; 1 BvR 263/08; 1 BvR 586/08),
in *https://www.bundesverfassungsgericht.de.*

Sentença de 27 de junho de 2018 (2 BvR 1405/17; 2 BvR 1780/17), in *https://www.bundesverfassungsgericht.de.Bundesgerichtshof*

Sentença de 24 de janeiro de 2001, in *Entscheidungen des Bundesgerichtshofes in Strafsachen,* 46, pp. 266 e ss., Carl Heymanns Verlag KG, Colónia e Berlim, 2002.

Espanha

Tribunal Supremo

Sentença n.º 6307/2009, in *www.poderjudicial.es.*

Estados Unidos

Supreme Court of the United States

Sentença United States v. Jones, in *http://supreme.justia.com* (consultado em 14/10/2023).

United States Court of Appeals

Sentença National City Trading Corp. v. United States, 635 F.2d 1020 (2nd Circuit, 1980), in *https://casetext.com/case/national-city-trading-corp-v-united-states-2* (consultado em 14/10/2023). *United States Court for the District of Vermont*

Sentença United States v. Hunter, 13 F. Supp. 2d 574 (1998), in *https://law.justia.com/cases/federal/district-courts/FSupp2/13/574/2311683/* (consultado em 14/10/2023).

[*] Professor Auxiliar da Universidade Europeia

(445) O presente texto retoma anteriores reflexões do autor – *Nos 20 anos da Carta Europeia dos Direitos Fundamentais: sobre a cultura dos direitos humanos como chão comum da União Europeia. Reflexões jurídico-políticas, em Privacy and Data Protection Magazine,* n.º 01, 2021, pp. 222 a 231; *Sobre a cultura europeia dos direitos: do (pretenso) chão comum à dinâmica de polarização,* em VV. AA, *Polarização – ensaios de História, Filosofia e Teoria política,* Alêtheia Editores, Lisboa, 2023 [no prelo].

(446) Curiosamente, ideias personalistas haviam já deixado a sua marca em ordens não liberais de entre guerras. Pense-se, por exemplo, no projeto constitucional assinado pelo Marechal Pétain no começo de 1944, em cujo artigo primeiro se declarava: «A liberdade e a dignidade da pessoa humana são valores supremos e bens intangíveis (...)». Tal documento acha-se reproduzido em Maurice Duverger, *Constitutions et Documents Politiques,* 6.ª edição, Presses Universitaires de France, Paris, 1971, pp. 167 a 176 *(«Project de Constitution du maréchal Pétain»).*

(447) No artigo 1.º, afirmava-se ainda: «Todos os seres humanos nascem livres e iguais em dignidade e em direitos». Consultámos versão do texto disponibilizada online pelo Centro de Informação das Nações Unidas em Portugal – https://www.cig.gov.pt/wp-content/uploads/2018/01/Declaracao-Universal-dos-Direitos-Humanos.pdf.

10 | SOBRE AS VISÕES CONTEMPORÂNEAS DOS DIREITOS FUNDAMENTAIS: ENTRE DIGNIDADE HUMANA, AUTODETERMINAÇÃO, COMUNIDADE E «EMENDA À TOTALIDADE»[445].

*Pedro Rebelo Botelho Alfaro Velez**

Resumo:

No texto que segue, procurar-se-á traçar um panorama das diversas culturas de direitos bem como das contraculturas alternativas atualmente existentes nas democracias ocidentais, no quadro europeu, sobretudo, mas também no contexto norte-americano.

Palavras-chave: direitos humanos; direitos fundamentais; autodeterminação; comunidade; catolicismo.

Nos parágrafos seguintes, tentar-se-á esboçar um panorama das hodiernas culturas de direitos bem como das contraculturas alternativas existentes nas democracias ocidentais, no caso europeu, sobretudo, mas abrangendo também o cenário norte-americano.

1. Os começos e os referentes «personalistas»

O segundo após guerra normalizou um específico discurso de direitos, girando em torno dos radicais éticos «dignidade humana» ou «dignidade da pessoa humana» ou «dignidade do ser humano» ou de «*dignidade de todos os membros da família humana*»[446]. Tenha-se em mente, desde logo, a Declaração Universal dos Direitos Humanos (1948): «Considerando que o reconhecimento da dignidade inerente a todos os membros da família humana e dos seus direitos iguais e inalienáveis constitui o fundamento da liberdade, da justiça e da paz no mundo», dizia-se e diz-se logo no primeiro considerando preambular (sublinhado nosso)[447]. Releve-se outros sim, para além dos Pactos Internacionais decorrentes dessa declaração – o de Direitos Civis e Políticos e o de Direitos Económicos, Sociais e Culturais (1966) – , um documento constitucional europeu paradigmático como a Lei Fundamental alemã de 1949, com o seu eloquente artigo 1.º: « (1) A dignidade humana será inviolável. Respeitá-la e protegê-la será dever de toda autoridade estatal.

(2) O povo alemão reconhece, portanto, os direitos humanos invioláveis e inalienáveis como a base de qualquer comunidade, da paz e da justiça no mundo.

(3) Os seguintes direitos básicos vincularão o legislativo, o executivo e o judiciário como lei diretamente aplicável»[448].

Mais contemporaneamente, várias vagas de formação constitucional inscrever-se-iam no mesmo solo ético-jurídico: as influentes constituições portuguesa de 1976 (artigos 1.º e 16.º, n.º 2)[449] e espanhola de 1978 (artigo 10.º)[450] são disso exemplo. A Carta Europeia dos Direitos Fundamentais (politicamente proclamada no ano 2000 – 7 de dezembro – e posteriormente elevada, numa versão adaptada, a um plano jurídico vinculativo, por força do Tratado de Lisboa, que entraria em vigor em 1 de dezembro 2009), sobre a qual se pretendeu erigir uma União política ancorada numa cultura compartilhada de direitos humanos, retomaria e proclamaria explicitamente um tal património ideacional: «Consciente do seu património espiritual e moral, a União baseia-se nos valores indivisíveis e universais da dignidade do ser humano, da liberdade, da igualdade e da solidariedade; assenta nos princípios da democracia e do Estado de direito»[451].

---

[448] Tradução nossa a partir de versão em inglês, disponibilizada pelo Ministério Federal da Justiça, em https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html].

[449] «Artigo 1.º (República Portuguesa)
Portugal é uma República soberana, baseada na dignidade da pessoa humana e na vontade popular e empenhada na construção de uma sociedade livre, justa e solidária.»

De acordo com o n.º 2 do artigo 16.º da CRP de 1976, «Os preceitos constitucionais e legais relativos aos direitos fundamentais devem ser interpretados e integrados de harmonia com a Declaração Universal dos Direitos do Homem».

[450] *«Artículo 10*
La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.

Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.» Ver https://app.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=10&fin=55&tipo=2.

[451] Consultámos o(s) texto(s) constante(s) do Jornal Oficial da União Europeia (edição em língua portuguesa).

Esteve (estará ainda?) em causa o reconhecimento de um certo mínimo ético fundacional (desde logo dos sistemas de direitos fundamentais): «a igualdade fundamental de todos» os seres humanos «numa humanidade comum»[452]. Contra um tal pano de fundo, se entende a emergência e a popularização, doutrinárias e jurisprudenciais, da célebre fórmula (de derivação kantiana) de Günther Dürig, vedando ao poder público tratar o ser humano concreto como mero objeto, coisificando-o.

O caráter vago e a originária ambivalência de um tal discurso de direitos têm sido notados. A Declaração Universal de 1948 não espelhou um «acordo filosófico» de fundo (sobre o que significam «a natureza, a pessoa humana e a sua dignidade»), mas tão-só um mero «acordo prático», como reconhecido pela Comissão da Unesco para as Bases Teóricas dos Direitos do Homem[453]. A Declaração parece, por outro lado, combinar, do ponto de vista da substância normativa, distintos registos axiológicos: um personalismo ("objetivista") com traços de jusnaturalismo clássico[454] e um outro mais eivado de subjetivismo[455].

---

[452] Ver Luís Pedro Pereira Coutinho, *Do que a República é: uma República baseada na Dignidade Humana,* Instituto de Ciências Jurídico-Políticas/Centro de Investigação de Direito Público; publicação disponível *online* – https://www.icjp.pt/sites/default/files/media/397-446.pdf . Cfr. também E.W. Böckenförde, *Human Dignity as a Normative Principle: Fundamental Rights in the Bioethics Debate* [2003] e *Will Human Dignity Remain Inviolable?* [2004], em E.W. Böckenförde, *Religion, Law, and Democracy, Selected Writings,* Oxford University Press, Oxford, 2020, pp. 339 a 353 e pp. 354 a 365, respetivamente.

[453] VV. AA., *Los derechos del hombre,* 4.º ed., Barcelona, Laia, 1976, pp. 389-411, *apud Estanislao* Cantero, *El realismo jurídico de Juan Vallet de Goytisolo,* Marcial Pons, Madrid, 2023, pp. 102 e 103.

[454] Atente-se, por exemplo, no artigo 16.º da Declaração:
«1. A partir da idade núbil, *o homem e a mulher têm o direito de casar e de constituir família,* sem restrição alguma de raça, nacionalidade ou religião. Durante o casamento e na altura da sua dissolução, ambos têm direitos iguais.

2. O casamento não pode ser celebrado sem o livre e pleno consentimento dos futuros esposos.

3. *A família é o elemento natural e fundamental da sociedade e tem direito à proteção desta e do Estado*» (sublinhados nossos).

[455] Tal parece ser o balanço global de Grégor Puppinck, em *Os Direitos do Homem Desnaturado,* Principia, Lisboa, 2019. Cfr. também Samuel Moyn, *Christian Human Rights,* University of Pennsylvania Press, Philadelphia, 2015, sublinhando «*the conservative Catholic influences on the mid-twentieth-century international human rights movement*» (nas palavras de um recensor da obra, John Witte, Jr). Sobre o(s) personalismo(s) em quadrantes cristãos, ver Gonzalo Ibáñez, *Persona y derecho en el pensamento de Berdiaeff, Mounier y Maritain,* Universidade Católica do Chile, Santiago do Chile, 1984. Cfr., em especial, de Jacques Maritain, *Les droits de l'homme et la loi naturelle,* Paul Hartmann, Paris, 1947. Para uma desconstrução das ideias personalistas, muito em especial as que presidiram à fundação da República italiana (Constituição de 1947), nelas vislumbrando instâncias de individualismo subjetivista (concebendo a pessoa sem natureza, como existência que se constrói a si mesma), ver, porém, Danilo Castellano, *L'ordine politico-giuridico «modulare» del personalismo contemporaneo,* Nápoles, Edizioni Scientifiche Italiane, Nápoles, 2007.

Daí também que distintas linhas de interpretação – dando corpo a diversas visões e culturas de direitos – se tivessem podido afirmar, referindo-se ou reconduzindo-se aos mesmos enunciados juslegitimadores, à partida abertos[456]. É o que se procurará ilustrar no que segue.

2. «Autodeterminação e direito»

> No mundo europeu, têm vindo a cristalizar novíssimos direitos ditos de autonomia ou de liberdade individual de escolha; direitos alcandorados a fundamentais, com incidência sobre as importantes e centrais dimensões antropológicas do começo e do fim da vida (humana), da configuração da família, da reprodução da espécie, da identidade corporal-sexual...Tudo representado como extensão do cânone "tradicional" dos direitos humanos, em nome de uma ideia de autodeterminação (da vontade) individual ou pessoal, num processo que se afigura ainda in fieri[457].
>
> A partir de 2001, foi-se caminhando em direção à consagração da figura do casamento entre pessoas do mesmo sexo (em 2001, a Holanda terá sido o primeiro país europeu a consagrar a figura, ano em que permitiu também a adoção por casais do mesmo sexo)[458].
>
> Alguns exemplos recentes da afirmação desta dinâmica político-jurídica afiguram-se eloquentes: pense-se nas decisões dos tribunais constitucionais italiano, alemão e austríaco no que tange à problemática do fim de vida. O tribunal constitucional alemão invocou explicitamente a existência de um «direito subjetivo à morte»[459]. Num mesmo cumprimento de onda, o presidente do tribunal constitucional austríaco

---

[456] Sobre a temática das várias hipóteses de leitura da «dignidade da pessoa humana», ver J. de M. Alexandrino, *Perfil constitucional da dignidade da pessoa humana: Um esboço traçado a partir da variedade de concepções, em Revista Brasileira De Direitos Fundamentais & Justiça,* 4 (11), 2010, pp. 13 a 38.

[457] Ver Rudi Di Marco, *Autodeterminazione e diritto,* Edizioni Scientifiche Italiane, Napoli, 2017.

[458] Ver, na *Wikipedia,* a entrada *Recognition of same-sex unions in Europe* (https://en.wikipedia.org/wiki/Recognition_of_same-sex_unions_in_Europe).

[459] Ver BVerfG, *Judgment of the Second Senate of 26 February 2020* – 2 BvR 2347/15 –, paras. 1-343, http://www.bverfg.de/e/rs20200226_2bvr234715en.html . Sobre a *sentenza n. 242/2019* do Tribunal Constitucional italiano, ver o comentário de Danilo Castellano e Rudi Di Marco, *Le motivazioni della Corte costituzionale sul suicídio assistito: ulteriore atto di "protezione dell'anarchia" da parte del giuspositivismo assoluto, em Filodiritto* (Filodiritto.com), 10 de dezembro 2019 (https://www.filodiritto.com/le-motivazioni-della-corte-costituzionale-sul-suicidio-assistito-ulteriore-atto-di-protezione-dellanarchia-da-parte-del-giuspositivismo-assoluto).

(Christoph Grabenwarter) sumariaria publicamente a doutrina subjacente à tomada de posição da jurisdição por si presidida: "A decisão plenamente consciente de cometer suicídio deve ser respeitada pelo legislador"[460].

As instituições da União Europeia não têm ficado imunes à expressão das notadas trajetórias. Algumas das áreas dos novos direitos individuais ditos de autonomia ou de liberdade de escolha constituirão, à partida, é certo, áreas de reserva estadual (direito da família, por exemplo). A realidade jurídico-política "final" afigura-se, porém, mais complexa; pense-se, por exemplo, em recentes iniciativas da Comissão Europeia, no tocante a várias áreas: à liberdade de circulação de "situações familiares" definidas em certos Estados, mas não reconhecidas noutros; ao alargamento das definições de discurso de ódio online abrangendo a «homofobia»; ao corte de fundos europeus às cidades polacas autoproclamadas zonas livres de ideologia LGBT(QIA+...)[461].

Ultimamente, o Parlamento Europeu tem vindo a tornar-se um lugar de afirmação da referida visão (ou decisão...) jusfundamental. Um momento parlamentar destes últimos tempos afigura-se particularmente eloquente: a aprovação de uma resolução «sobre a abolição de facto do direito ao aborto na Polónia» (sic), condenando a decisão do Tribunal Constitucional polaco que veio considerar inconstitucional uma das poucas indicações

---

[460] Por decisão de 11 de dezembro de 2020, o referido tribunal considerou inconstitucional a regra da lei penal austríaca criminalizadora da assistência ao suicídio (por incorrer em violação da autodeterminação individual), tendo a referida decisão constituído o legislador na obrigação de regular a matéria até ao final de 2021. Ver https://www.jurist.org/news/2020/12/austria-constitutional-court-strikes-down-ban-on-assisted-death/ .

[461] Ver Charlemagne/The rainbow curtain, em The Economist, 21 de novembro de 2020, p. 24. Em relação à primeira das apontadas áreas objeto de iniciativa da Comissão, cumpre registar que o Tribunal de Justiça europeu teve já ocasião de nela entrar. Embora reconhecendo caber aos Estados Membros da União Europeia dispor sobre a definição do casamento, o Tribunal decidiu (5 de junho de 2018), porém, que «o nacional de um Estado terceiro, do mesmo sexo do cidadão da União e cujo casamento com este último foi celebrado num Estado-Membro em conformidade com o direito deste, dispõe de um direito de residência superior a três meses no território do Estado-Membro de que o cidadão da União é nacional». Segundo o Tribunal, a expressão cônjuge seria, no direito europeu chamado à colação, «neutro do ponto de vista do género». O acórdão em causa pode ser visto em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130dab49a6e70cfd42a3a61c9d52c93df497.e34KaxiLc3eQc40LaxqMbN4Pb3mLe0?text=&docid=202542&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=134584.

legais justificadoras do abortamento no ordenamento daquele país (deficiência fetal, indicação julgada legalizadora de práticas de «eugenia liberal»). A resolução estriba-se num reconhecimento explícito de um direito ao aborto como direito fundamental internacionalmente reconhecido (no âmbito dos direitos sexuais e reprodutivos)[462].

Em amplos setores das classes político-mediáticas europeias, chega-se hoje ao ponto culminante de (meta)decretar como inquestionáveis estes novíssimos direitos de autodeterminação individual. O que talvez signifique um brutal estreitamento do campo das discussões e deliberações públicas e políticas tidas como razoáveis.

3. As qualificações nacionais-comunitárias

Não obstante, em alguns países do continente europeu, assistimos à emergência de projetos político-constitucionais apontando para uma (re)ancoragem do discurso de direitos num certo ethos nacional-comunitário de formação cristã, ligando «dignidade humana» a «dignidade nacional» ou do «modo de vida nacional».

Na Hungria, parece estar *in fieri* a construção de uma ordem político-constitucional que tende a fundar-se explicitamente numa «ortodoxia pública» com o referido sentido. A nova constituição húngara de 2011 é precedida de uma *invocatio Dei* – «Deus abençoe os Húngaros» – e de uma preambular «Confissão Nacional» *(sic)* evocando uma Nação concebida como unidade cultural intemporal de definição cristã; Confissão Nacional essa erigida a contexto interpretativo das concretas disposições constitucionais [artigo R (3)] Algumas disposições constitucionais afiguram-se particularmente significativas – assim, segundo o artigo L (1): «A Hungria protegerá a instituição do casamento como a união entre um homem e uma mulher estabelecida por decisão voluntária, e a família como a base da sobrevivência da nação»; segundo o Artigo II:

[462] VA resolução está disponível em: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2876(RSP)&l=en

«(A dignidade humana é inviolável.) Todo o ser humano tem direito à vida e à dignidade humana; a vida embrionária e fetal devem ser objeto de proteção desde o momento da conceção»[463].

Na Polónia, um horizonte político-constitucional similar (reatando hipóteses de estruturação político-constitucional debatidas no pós-queda do império soviético) não será estranho ao campo conservador polaco[464]. A respeito deste último país, é interessante registar que uma administração conservadora, em reação ao que entendeu serem os elementos de pendor "liberal-progressista" incorporados na Carta Europeia dos Direitos Fundamentais, negociou com sucesso a inclusão do Estado polaco num protocolo ao Tratado de Lisboa relacionado com a aplicação da Carta (prevalecendo-se de um dispositivo originalmente desenhado para o caso britânico e visando garantir a não sobre extensão da jurisdição do Tribunal de Justiça da União Europeia; e cujas precisas implicações jurídicas têm sido discutidas, na doutrina e na jurisprudência)[465].

4. O discurso de direitos católico

Já nos anos noventa, uma relevante contraposição entre o discurso católico dos direitos humanos – especialmente desenvolvido pelo Papa João Paulo II – e as interpretações seculares dos direitos humanos se tinha tornado eminentemente patente na vida político-constitucional de certas comunidades políticas europeias[466].

---

[463] Consultámos edição em inglês do Ministério da Justiça húngaro (2019).

[464] Para uma crítica global à presente ordem ocidental, provinda do campo conservador polaco, ver, de Ryszard Legutko, *The Demon in Democracy: Totalitarian Temptations in Free Societies.* Encounter Books, New York, NY., 2016 (devolvendo acusações de "iliberalismo" às democracias ocidentais, que hoje veiculariam uma forma mental totalizante...).

[465] *Protocolo (n.º 30) relativo à aplicação da Carta dos Direitos Fundamentais da União Europeia à Polónia e ao Reino Unido.* Ver, na *Wikipedia,* a entrada *Charter of Fundamental Rights of the European Union* (https://en.wikipedia.org/wiki/Charter_of_Fundamental_Rights_of_the_European_Union).

[466] Sobre essa contraposição ver Gustavo Zagrebelsky, *El derecho dúctil, Ley, derechos, justicia,* trad., 10.ª ed., Editorial Trotta, Madrid, 2011, pp. 75 e ss. [Tradução espanhola de obra italiana dos anos 90 que rapidamente adquiriu o estatuto de um clássico].

Efetivamente, de Leão XIII aos nossos dias, num percurso em que foram marcos centrais a elaboração por Pio XII de um "catálogo" de «direitos fundamentais da pessoa» e, sobretudo, o ensinamento de João XXIII, *máxime* na encíclica *Pacem in Terris* de 1963 (elaborando de modo orgânico-sistemático um discurso católico sobre os direitos do homem), bem como os documentos do Concílio Vaticano II (*Gaudium et Spes,* «sobre a Igreja no mundo atual»; *Dignitatis Humanae,* «sobre a liberdade religiosa»), foi-se desenvolvendo, no magistério da Igreja Católica, a tentativa de dissociar o discurso de direitos dos seus pressupostos filosóficos ou ideológicos modernos e iluministas, reconduzindo-o a uma base objetivista-teleológica ou integrando num quadro objetivista-teleológico[467].

5. As propostas de «emenda à totalidade»

No universo católico, certas vozes sugerem, no entanto, que o discurso de direitos humanos e fundamentais de derivação liberal requer «uma emenda à totalidade», devendo, pois, ser abandonado, na medida em que manifestada uma noção de «*liberdade negativa*»: uma liberdade individual tendo apenas como critério ou como regra a própria liberdade; ou seja, uma liberdade sem regra substantiva intrínseca[468].

Na área do pensamento tradicionalista hispânico, que hoje conhece uma nova e cada vez mais visível vaga de produção teórica, defende-se explicitamente uma reconstrução alternativa do político-constitucional em outras bases, na lei e no direito naturais catolicamente entendidos[469].

---

[467] Ver, para maiores aprofundamentos, Pedro Velez, O *"Espírito Dominicano" No Pensamento Político-Constitucional Ocidental: Algumas Notas, em Privacy and Data Protection Magazine: revista científica na área Jurídica,* n.º 03, 2021, pp. 69 a 81.

[468] Ver, neste sentido, Danilo Castellano, *Introducción a la filosofía de la política: Breve manual,* Marcial Pons, Madrid, 2020, pp. 113 e ss.

[469] Ver Juan Manuel de Prada, *Una enmienda a la totalidad: El pensamiento tradicional contra las ideologías modernas,* Homo Legens, Madrid, 2022; Miguel Ayuso, *Tradición política e hispanidad,* Consejo de Estudios Hispánicos Felipe II, Madrid, 2020; Miguel Ayuso, *La constitución cristiana de los Estados,* Ediciones Scire, Barcelona, 2008. Cfr. também Juan Fernando Segovia, *Los Derechos Humanos, Individualismo, personalismo y antinaturalismo,* Marcial Pons, Madrid, 2022.

Aos direitos humanos contrapõe-se uma noção clássica-cristã de dignidade humana[470].

Em outros quadrantes cristãos, não necessariamente católicos, detetam-se orientações afins: no seio do influente movimento de génese britânica autodenominado *radical orthodoxy*[471], propõe-se a superação de «*subjective rights as 'possessive individualism'*» dando lugar a «*classical objectivist notions of justice as 'right order'*»[472].

6. Os vários discursos americanos

Tal como no contexto europeu, também em solo americano cristalizou, porventura a partir de um outro circunstancialismo de base[473], um discurso de direitos – que tem sido um discurso de alargamento de direitos – girando em torno de uma certa compreensão de liberdade como autodefinição e autoexpressão do indivíduo. A conceção afirmada pelo Supremo Tribunal, a título de fundamento, em casos emblemáticos como *Planned Parenthood of Southeastern Pennsylvania v. Casey* (de 1992) – «*At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life*»[474]; ou *Obergefell v. Hodges* (2015) – «*The Constitution promises liberty to all within its reach, a liberty that includes certain specific rights that allow persons, within a lawful realm, to define and express their identity*»[475].

---

[470] Cfr. José Miguel Gambra, *La noción clásica de dignidad y los derechos humanos,* em *Anales de la Fundación Francisco Elías de Tejada,* Nº. 16, 2010, págs. 31 a 54.

[471] Movimento teológico e filosófico, reunindo vozes anglo-católicas e romano-católicas, gerado no meio universitário do Reino Unido. Veja-se John Milbank e Simon Olivier (eds.), *The Radical Orthodoxy Reader,* Routledge, London/New York, 2009.

[472] Ver John Milbank, *Against Human Rights: Liberty in the Western Tradition,* em *Oxford Journal of Law and Religion,* Volume 1, N.º 1, 2012, pp. 203–234.

[473] Não obstante, tenha-se em mente o envolvimento americano (Eleanor Roosevelt) na gestação da Declaração Universal dos Direitos Humanos (1948).

[474] Ver https://supreme.justia.com/cases/federal/us/505/833/case.pdf.

[475] Ver https://www.supremecourt.gov/opinions/14pdf/14-556_3204.pdf. A natureza revolucionária da decisão do Tribunal levaria mesmo o célebre juiz Scalia a proclamar, em voto de vencido no referido caso, «*no social transformation without representation*». Sobre o pensamento jurídico-constitucional de Scalia, ver Robert P. George, *Antonin Scalia: An American Originalist,* em *Public Discourse,* 16. fev. 2016 (disponível em https://www.thepublicdiscourse.com/2016/02/16478/).

Em contraponto, não deixaram de se afirmar sensibilidades político-jurídicas de orientação originalista ("historicista-americana") e/ou de pendor jusnaturalista[476]. A título de ilustração, tenha-se em conta o teor do trabalho produzido pela comissão estabelecida, há poucos anos, no âmbito Departamento de Estado – comissão liderada pela ilustre professora de direito e ex-embaixadora dos EUA junto da Santa Sé, a católica Mary Ann Glendon. Aí se sugere uma refundamentação do discurso dos direitos na lei natural – fala-se de «direitos objetiva e universalmente verdadeiros», por exemplo – , bem como uma depuração do catálogo de direitos fundamentais (insistindo-se em direitos tidos por essenciais ou primordiais – liberdade religiosa; propriedade); afastando-se outrossim um ideal de universalização-abstrata dos mesmos[477].

À hegemonia de um discurso de direitos têm alguns contraposto a desejabilidade de um aumento do espaço de deliberação política no que toca a questões atual e potencialmente fraturantes, designadamente em termos de um novo protagonismo das esferas públicas e políticas dos Estados federados[478]. A recentíssima decisão do Supremo Tribunal Americano em *Dobbs v. Jackson Women's Health Organization* (2022)[479], negando, com impacto histórico-mundial, a doutrina estabelecida em *Roe v. Wade* (1973) e reiterada em *Planned Parenthood v. Casey* (1992) [existência de um direito constitucional ao aborto], parece ter querido abrir um tal caminho.

---

(476) No discurso jurídico académico, ver, por exemplo, na revista Public Discourse (jornal online do "conservador" *Witherspoon Institute* – Princeton, New Jersey): Carson Holloway, In *Defense of Originalism*, 3 de abril de 2018 (https://www.thepublicdiscourse.com/2018/04/21097/) e, combinado as duas posições mencionadas no corpo do texto, Gerard V. Bradley, *Moral Truth and Constitutional Conservatism*, 10 fev. 2020 (https://www.thepublicdiscourse.com/2020/02/60037/).

(477) Ver Commission on Unalienable Rights, *Report of the Commission on Unalienable Rights*, U.S. Department of State, 2020 (https://www.state.gov/report-of-the-commission-on-unalienable-rights/)

(478) Ver Peter J. Leithart, *Is federalism the solution?*, em *First Things*, 11. 6. 20 (https://www.firstthings.com/web-exclusives/2020/11/is-federalism-the-solution).

(479) Ver https://supreme.justia.com/cases/federal/us/597/19-1392/case.pdf .

Também nos EUA certas vozes parecem sugerir a superação de uma ordem constitucional *rights-based*, via refundação da ordem constitucional, em direção a «novos modos e ordens»:

Atente-se, por exemplo, no já célebre livro de Patrick J. Deneen, intitulado «*Why Liberalism failed*», descodificando o Estado Liberal como Estado Totalizante e sugerindo toquevilianamente que a ordem política deverá ser reconstruída a partir de horizontes comunitários de índole local[480].

Um outro filão crítico vai mais longe: a um Estado Secular tido por dissolvente da Ordem só conviria contrapor um desejável regresso ao paradigma do Estado Confessional Católico. Referimo-nos ao autodenominado «integralismo», movimento de elite de pendor académico, mas cada vez mais discutido no espaço público[481]. Embora sem impugnar a verdade das liberdades e separações modernas, alguns intelectuais públicos sugerem a possibilidade de (re)ancorar a ordem constitucional num ethos clássico-cristão, num (re)enraizamento cultural a ser forjado de baixo para cima, num modo não autoritário-coercitivo[482].

[480] Patrick J. Deneen, *Why liberalism failed*, Yale University Press, New Haven, 2018.

[481] Para uma defesa desta posição, ver Thomas Pink, *Integralism, Political Philosophy, and the State*, em *Public Discourse*, 09.05.2020 (https://www.thepublicdiscourse.com/2020/05/63226/).

[482] Ross Douthat, Gentler Christendom, em *First Things*, Junho 2022 (https://www.firstthings.com/article/2022/06/a-gentler-christendom).

11 | A GOVERNAÇÃO E A REUTILIZAÇÃO DE DADOS CONTIDOS EM DOCUMENTOS ADMINISTRATIVOS E A PROTEÇÃO DE DADOS PESSOAIS NA LEGISLAÇÃO PORTUGUESA E NO DIREITO DA UNIÃO EUROPEIA

*Alexandre Sousa Pinheiro**

Resumo

O presente texto baseia-se na evolução do mercado de dados europeu, no contexto de uma estratégia de dados da UE. Neste contexto, identificamos as fontes normativas europeias e nacionais relevantes para compreender o conceito de reutilização perante dados pessoais ou dados não pessoais. A aplicação do *RGPD* e a sua conciliação com as diversas formas de extrair informação constitui uma base essencial do trabalho. Compete avaliar os serviços de intermediação de dados e os seus conceitos naturais.

Palavras-chave:

Proteção de dados pessoais; Proteção de dados não pessoais, reutilização de dados; dados abertos; serviço de intermediação de dados; partilha de dados; utentes de dados e detentores de dados.

1. Enquadramento das fontes

1.1. Origem e desenvolvimento normativo

Apesar de a Diretiva 2003/98/CE do Parlamento Europeu e do Conselho de 17 de novembro de 2003 relativa à reutilização de informações do sector público[483] ser indicada como instrumento jurídico fundador da regulação da matéria na União Europeia, deve considerar-se a influência de outros instrumentos normativos, como a Diretiva do Conselho 90/313/CEE, de 7 de junho de 1990, relativa à liberdade de acesso à informação em matéria de ambiente.

---

* Professor Auxiliar da Universidade Europeia. Membro da CADA.

(483) Transposta para o Direito português pela Lei n.º 46/2007, de 24 de agosto, revogada pela Lei n.º 26/2016, de 22 de agosto, a atual Lei de Acesso aos Documentos Administrativos – LADA, onde permanece a transposição, com alterações posteriores.

A própria Diretiva de 2003 faz referência no *Considerando* (2) à Diretiva 90/313/CEE: "(…) relativa à liberdade de acesso à informação em matéria de ambiente iniciou um processo de mudança na forma como as entidades públicas abordam a questão da abertura e da transparência, estabelecendo medidas para o exercício do direito de acesso do público à informação sobre ambiente, que deve ser impulsionado e prosseguido".

A Diretiva 90/313/CEE foi revogada pela Diretiva de 2003, não só para ampliar ao acesso à informação administrativa, como, também, para eliminar as disparidades existentes no acesso à informação entre os diversos Estados-Membros.

1.2. Os aspetos que merecem especial atenção previstos na Diretiva 2003/98/CE, e que influenciaram a futura legislação da UE sobre o acesso e tratamento da informação administrativa respeitam, nomeadamente, aos seguintes aspetos:

i) Previsão do princípio geral da reutilização dos documentos na posse do sector público, garante a reutilização de documentos na posse de organismos do sector público, sempre que permitida, e a disponibilização da informação através de meios eletrónicos (artigo 3.º);

ii) Ausência de os Estados-Membros autorizarem a reutilização de documentos e não continha regulação sobre o direito de acesso a documentos administrativos, que alterasse a legislação nacional (Considerando 9);

iii) Disponibilização dos documentos em qualquer formato ou linguagem que já existam, sempre que possível e adequado, preferencialmente através de meios eletrónicos (artigo 5.º, n.º 1);

iv) Os emolumentos não poderiam exceder o custo da sua recolha, produção, reprodução e divulgação, acrescido de uma rentabilidade razoável para o investimento (artigo 6.º);

v) As condições aplicáveis à reutilização de documentos não deviam ser discriminatórias para categorias de reutilização equivalentes (artigo 10.º, n.º 1);

vi) A Diretiva de 2003, devia ser aplicada e executada cumprindo a Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (*Considerando* 21);

vii) Os direitos de propriedade intelectual de terceiros não seriam afetados pela Diretiva, bem como os direitos de propriedade industrial (*Considerando* 22).

1.2.1. A Diretiva de 2003 foi alterada pela Diretiva 2013/37/EU de 26 de junho de 2013, enunciando-se como explicação geral da modificação que o regime jurídico de 2003 já estava superado pela evolução tecnológica, existindo "o risco de se perderem as oportunidades económicas e sociais proporcionadas pela reutilização dos dados públicos" (*Considerando* 5).

As alterações fundamentais introduzidas pela Diretiva de 2013, basearam-se em um sistema de "reutilização regra", salvas as exceções legislativamente previstas e tendendo a adquirir um caráter restritivo.

O princípio geral do artigo 3.º deixa de fazer depender a reutilização de normas permissivas, antes estabelece a regra de que os Estados Membros devem assegurar que os documentos a que se refere a Diretiva são reutilizáveis para fins comerciais ou não comerciais, salvo normas excecionais[484].

Na alteração ao artigo 4.º, n.º 4 da Diretiva de 2003, inseriram-se vias de recurso, em caso de indeferimento, após solicitação de reutilização de informação administrativa, que podem ter a natureza de organismo imparcial de recurso, de autoridade nacional

[484] *Considerando* (8) A Diretiva 2003/98/CE deverá ser alterada de modo a estabelecer claramente a obrigação, para os Estados-Membros, de tornar reutilizáveis todos os documentos, exceto se o acesso for restrito ou vedado ao abrigo de regras nacionais sobre acesso a documentos e sem prejuízo das outras exceções previstas na presente diretiva. As alterações introduzidas pela presente diretiva não visam definir ou alterar regimes de acesso nos Estados-Membros, os quais continuam a ser da sua responsabilidade."

da concorrência, de autoridade nacional de acesso a documentos ou uma autoridade judicial nacional[485].

A transposição da Diretiva de 2013 para o ordenamento jurídico português, atribuiu a competência para receber queixas à Comissão de Acesso aos Documentos Administrativos (CADA) prevista no artigo 22.º, n.º 1, alínea b) da LADA.

Foram aprovadas, também, alterações que aqui não analisaremos, respeitando a formatos e a emolumentos.

Relevam também, no tema que tratamos, os seguintes Pareceres do Grupo de Trabalho do artigo 29.º: (i) Parecer n.º 3/99, sobre preservação de dados de tráfico de ISPs para finalidades de *law enforcement*[486]; (ii) Parecer n.º 5/2001, sobre o Relatório Especial do Provedor de Justiça Europeu ao Parlamento Europeu na sequência do projeto de recomendação à Comissão Europeia relativo à reclamação 713/98/IJH[487]; (iii) Parecer n.º 7/2003[488], sobre a reutilização da informação do sector público e proteção dos dados pessoais – Estabelecer um equilíbrio.

---

(485) *Considerando* (28) Esse organismo deverá ser organizado de acordo com os sistemas constitucionais e legais dos Estados-Membros e não deverá prejudicar quaisquer vias de recurso distintas de que os requerentes de reutilização dispõem. No entanto, esse organismo deverá ser diferente do mecanismo do Estado-Membro que estabelece os critérios para cobrar emolumentos superiores aos custos marginais."

(486) Grupo de Trabalho do artigo 29.º, 5085/99/EN/FINAL WP 25, 7 de setembro de 1999.

(487) Grupo de Trabalho do artigo 29.º, 5003/00/EN/Final WP 44, 17 de maio de 2001.

(488) Grupo de Trabalho do artigo 29.º, 10936/03/PT WP 83, 12 de dezembro de 2003.

De acordo com as conclusões do Parecer: "A questão de saber se a diretiva [Diretiva 95/46/CE] sobre proteção de dados autoriza a reutilização de informação proveniente do sector público que inclui dados pessoais carece de uma avaliação cuidadosa e casuística que permita estabelecer um equilíbrio entre o direito à proteção da vida privada e o direito de acesso público. Os organismos do sector público terão que considerar a legitimidade da comunicação relativamente a cada caso concreto, de acordo com os critérios fixados na diretiva. Dado que a análise do princípio de finalidades é crucial neste contexto, o presente parecer apresenta vários elementos que terão que ser considerados nessa análise. Caso a comunicação seja prevista, os organismos do sector público terão que observar os direitos das pessoas em causa, como o direito de informação ou de oposição, em particular se os dados se destinarem a ser reutilizados para fins comerciais, como o marketing direto, por exemplo". Esta posição do Grupo do Artigo 29.º não refere expressamente o consentimento (também não o exclui, evidentemente), admitindo outras fontes de legitimidade. O princípio da finalidade constitui a limitação fundamental da reutilização de documentos administrativos que contenham dados pessoais.

1.2.2. A Diretiva 2019/1024 de 20 de junho de 2019, transposta pela Lei n.º 68/2021, de 26 de agosto[489] , e que se integra na LADA (artigo 1.º, n.º 2) revogou a Diretiva 2003/98/CE[490], com a última redação com efeitos a partir de 17 de julho de 2021 (artigo 19.º) e introduziu importantes modificações no tema da reutilização tal como o estamos a tratar[491].

Algumas destas alterações extraem-se, nomeadamente, do *Considerando* (4):

(i) Disponibilização de acesso a dados dinâmicos em tempo real;

(ii) Permitir a reutilização de dados de empresas públicas[492], de organismos que realizam investigação e de organismos financiadores de investigação;

(iii) Evitar novos acordos de exclusividade.

---

[489] Com Declaração de Retificação n.º 31/2021, de 20 de setembro, publicado no DRE (Série I), de 26 de agosto de 2021.

[490] É igualmente revogada a Diretiva 2013/37 (artigo 19.º conjugado com o Anexo II).

[491] No Considerando (8) é apresentado o enquadramento da Diretiva: "O setor público dos Estados-Membros recolhe, produz, reproduz e divulga um largo espectro de informações em muitas áreas de atividade, como informações sociais, políticas, económicas, jurídicas, geográficas, ambientais, meteorológicas, sismológicas, turísticas, empresariais e sobre patentes e educacionais. Os documentos produzidos pelos organismos do setor público de natureza executiva, legislativa ou judicial constituem um conjunto de recursos vasto, variado e valioso que pode beneficiar a sociedade. A disponibilização dessas informações, o que inclui os dados dinâmicos, num formato eletrónico comum permite que os cidadãos e as entidades jurídicas encontrem novas maneiras de as utilizar e criem novos produtos e serviços inovadores. Nos seus esforços para tornar os dados facilmente disponíveis para reutilização, os Estados-Membros e os organismos do setor público podem ter a possibilidade de beneficiar de apoio financeiro adequado dos fundos e programas pertinentes da União e de receber esse apoio, assegurando uma ampla utilização de tecnologias digitais ou a transformação digital da administração pública e dos serviços públicos."

[492] "(*Considerando* 20) As empresas públicas recolhem, produzem, reproduzem e divulgam documentos para prestar serviços de interesse geral. A utilização de tais documentos para outros fins constitui uma reutilização. As políticas dos Estados-Membros podem ir além das normas mínimas estabelecidas na presente diretiva, permitindo assim uma reutilização mais alargada. Ao transporem a presente diretiva, os Estados-Membros poderão utilizar outros termos que não o termo «documentos», desde que mantenham integralmente o âmbito de aplicação do que é abrangido pela definição do termo «documento» na presente diretiva."

Os dados dinâmicos previstos no artigo 2.º, n.º 8 da Diretiva são transpostos para o Direito português no artigo 3.º, alínea k) da LADA:

«"Dados dinâmicos", documentos ou dados em formato digital, sujeitos a atualizações frequentes ou em tempo real, em particular devido à sua volatilidade ou rápida obsolescência, como os dados gerados por sensores.»

Os dados dinâmicos, levando em conta o *Considerando* (31) da Diretiva de 2019, respeitam, por exemplo a informação: ambiental; sobre o tráfego; de satélite; meteorológica e gerada por sensores.

Estas informações podem ter utilizações variadas quer no plano público, quer na vertente privada. Assim, informações meteorológicas atualizadas podem ter um valor significativo em áreas como a agricultura, mas podem igualmente ser decisivas em componentes públicas como as referentes à proteção civil.

No que tange à mobilidade, informações atualizadas sobre matéria de tráfego podem ser decisivas para a criação de políticas públicas na área dos transportes com repercussão, em especial, nas áreas metropolitanas.

O *Considerando* distingue entre a disponibilização imediata de dados ou após a sua alteração por via de uma interface de programação de aplicações (IPA), mais frequentemente designada pelo acrónimo saxónico API (application programming interface). O *Considerando* (32) ocupa-se de uma qualificação de "IPA" simples e tecnicamente descritiva: "(...) é um conjunto de funções, procedimentos, definições e protocolos que permite a comunicação máquina-máquina e o intercâmbio contínuo de dados."

O artigo 19-A da LADA, prevê, no seu n.º 1, transpondo o artigo 5.º, números 5 e 6, da Diretiva de 2019, que os órgãos e entidades da Administração Pública disponibilizam dados dinâmicos para reutilização imediatamente após a respetiva recolha, através de IPA[493] adequado e sempre que se justifique, sob a forma de descarregamento em bloco. O n.º 2 admite limites à disponibilização imediata.

---

[493] Cumpre sublinhar que, nos termos da Resolução do Conselho de Ministros n.º 131/2021, de 10 de setembro, sobre a "Estratégia para a Transformação Digital da Administração Pública 2021-2026 e o respetivo Plano de Ação Transversal para a legislatura", na Linha Estratégica III relativa a "arquiteturas de referência" existe o objetivo, indicado para 2022, de disponibilizar na Plataforma de Interoperabilidade da AP (iAP) um catálogo de IPAs.

O n.º 3 determina que os dados abertos devam ser disponibilizados em catálogos de IPAs no portal dados.gov[494]. A responsabilidade pelo portal compete à Agência da Modernização Administrativa (AMA)[495]. As características do citado portal estão enunciadas no artigo 27.º, n.º 5 da LADA:

"O portal dados.gov constitui-se como o catálogo central de dados abertos em Portugal, tendo como função agregar, referenciar, publicar e alojar dados abertos de diferentes organismos e setores da Administração Pública central, regional e local, funcionando também como um portal indexador de conteúdos alojados noutros portais ou catálogos de dados abertos, setoriais ou descentralizados (...)"

Os desenvolvimentos no acesso e reutilização de dados abertos – através do portal dados.gov – devem ser fundamento para o desenvolvimento de políticas públicas; basear-se num portal tecnologicamente evoluído e fomentar que as entidades públicas partilhem cada vez mais informação[496-497].

No âmbito da União Europeia (UE) pode verificar-se, também, acesso ao Portal de Dados Abertos[498].

---

[494] Sobre a sua caracterização, ver: https://dados.gov.pt/pt/docs/about_dadosgov/. O portal tem como função: "Além de funcionar como um serviço partilhado de alojamento e publicação de dados, que pode ser utilizado por qualquer organismo público, funciona também como um portal indexador de conteúdos alojados noutros portais/catálogos de dados abertos, sejam setoriais (ex. Saúde, Justiça, Ambiente) ou locais (ex. Municípios)".

[495] Pode consultar-se documentação contemporânea da Diretiva de 2016 aprovada pela AMA: https://www.ama.gov.pt/documents/24077/24804/guia_dados_abertos_ama.pdfN e https://www.ama.gov.pt/documents/24077/24804/guia_introdu__o_dados_abertos_ama.pdf/.

[496] Nuno Xavier e Gabriel Osório de Barros, "Em análise dados abertos em Portugal", Gabinete de Estratégia e Estudos, data 21-11-2022, disponível em: https://www.gee.gov.pt/pt/estudos-e-seminarios/artigos-category/32493-em-analise-dados-abertos-em-portugal?highlight=WyJkYWRvcyIsImFiZXJ0b3MiLCJkYWRvcyBhYmVydG9zIl0=, p. 10.

[497] No *Considerando* (11) da Diretiva de 2019 afirma-se que: "A evolução para uma sociedade baseada em dados, caso sejam utilizados dados provenientes de diferentes domínios e atividades, influencia a vida de todos os cidadãos da União, permitindo-lhes, nomeadamente, obter novos meios de acesso e aquisição de conhecimento".

[498] Disponível em: https://www.europeandataportal.eu/pt/using-data/use-cases

Apesar do conteúdo do artigo 19-A da LADA importa sublinhar que os conceitos de dados dinâmicos e dados abertos não se confundem. Os dados dinâmicos são uma categoria de dados abertos, tendo estes um alcance mais vasto[499].

1.2.2.1. Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia (RLFD).

Faremos uma análise sobre a relação entre o RLFD e o *RGPD*, especialmente no que respeita ao "conjunto de dados compostos por dados pessoais e não pessoais" (artigo 1.º, n.º 2 do RLFD) e referiremos as principais causas que levaram à aprovação do RLFD. Para além do instrumento normativo, será considerada a Comunicação da Comissão ao Parlamento Europeu e ao Conselho: Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados (COM (2019) 250, de 29.05.2019).

Na base do RLFD está a evolução da economia baseada nos dados – e respetivas "cadeias de valor"[500] – atendendo a uma dimensão cada vez mais digital, que tem como uma das consequências o desenvolvimento da "reutilização"[501].

---

[499] No articulado da Diretiva de 2019 não se encontra definição de dados abertos, ao contrário do que consta no Considerando (16) que, de uma forma pouco exata, os caracteriza como: "dados em formato aberto que idealmente podem ser utilizados, reutilizados e partilhados de forma livre por qualquer pessoa e para qualquer finalidade. As políticas de livre acesso aos dados, que incentivam a ampla disponibilização e a reutilização das informações do setor público para fins privados ou comerciais, com poucas ou nenhumas restrições legais, técnicas ou financeiras, e que promovem a circulação das informações, não só para os agentes económicos mas fundamentalmente para o público em geral (...)".

[500] *Considerando* (2): "As cadeias de valor de dados assentam em diferentes atividades relacionadas com os dados: criação e recolha de dados; agregação e organização de dados; tratamento de dados; análise, comercialização e distribuição de dados; utilização e reutilização de dados. O funcionamento eficaz e eficiente do tratamento de dados constitui um alicerce fundamental em todas as cadeias de valor de dados.".

[501] *Considerando* (1): "(...) O setor das tecnologias da informação e das comunicações deixou de ser um setor específico, passando a ser a base de todos os sistemas económicos e de todas as sociedades modernas e inovadoras. Os dados eletrónicos são um elemento central desses sistemas e podem gerar muito valor quando analisados ou combinados com serviços e produtos. Por outro lado, o rápido desenvolvimento da economia dos dados e das tecnologias emergentes, como a inteligência artificial, os produtos e serviços ligados à internet das coisas, os sistemas autónomos e a 5G, suscitam novos problemas jurídicos em torno das questões do acesso aos dados, da reutilização dos dados, da responsabilidade, da ética e da solidariedade".

Para garantir a fluidez da economia digital, o RLFD cria "segurança jurídica para que as empresas possam escolher onde pretendem tratar os seus dados na UE, aumenta a confiança nos serviços de tratamento de dados e contraria as práticas de vinculação a um prestador de serviços"[502].

Como já referimos, uma das matérias importantes a tratar na análise do RLFD consiste na distinção entre dados não pessoais e dados pessoais. Deve, no entanto, reconhecer-se as vantagens dos fluxos de dados independentemente da sua natureza, para a liberdade de particulares e empresas – no "grande mercado da UE" – integrados numa economia digital de mercado único[503].

[502] (COM (2019) 250), p. 2.

Para garantia da concorrência e da segurança dos dados especialmente no plano transfronteiriço, importa referir o extenso tratamento que o RLFD concede à portabilidade. Introdutoriamente, ver *Considerando* (29).

[503] "(...) os dados podem circular livremente entre os Estados-Membros, permitindo aos utilizadores de serviços de tratamento de dados utilizar os dados recolhidos em diferentes mercados da UE para melhorar a sua produtividade e competitividade. Os utilizadores podem, assim, tirar pleno partido das economias de escala proporcionadas pelo grande mercado da UE, melhorando a sua competitividade a nível mundial e aumentando a interconectividade da economia europeia dos dados". *Ibidem*.

De acordo com o *Considerando* (10): "Nos termos do Regulamento (UE) 2016/679, os Estados-Membros não podem restringir nem proibir a livre circulação de dados pessoais no interior da União por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais. O presente regulamento estabelece o mesmo princípio de livre circulação no interior da União relativamente aos dados não pessoais, com exceção dos casos em que se justifique uma restrição ou uma proibição por motivos de segurança pública. *O Regulamento (UE) 2016/679 e o presente regulamento estabelecem um conjunto coerente de regras que preveem a livre circulação de diferentes tipos de dados. Por outro lado, o presente regulamento não impõe a obrigação de armazenar separadamente os diferentes tipos de dados.*".

1.2.2.1.1. O RLFD distingue entre dados pessoais, mantendo a definição prevista no artigo 4.º, n.º 1 do *RGPD* (artigo 3.º, n.º 1)[504] , dados não pessoais – ou seja, informação que não contenha dados pessoais[505] – e a conjuntos de dados compostos por dados pessoais e não pessoais (artigo 2.º, n.º 2). O RLFD refere ainda, os conjuntos de dados compostos por dados pessoais e não pessoais indissociavelmente ligados (artigo 2.º, n.º 2).

A aplicação do RLFD verifica-se quanto a dados não pessoais, valendo o *RGPD* no que tange a dados pessoais, particularmente, os constantes de conjuntos de dados compostos. O RLFD sublinha essa solução no caso de dados anonimizados – considerados como dados não pessoais – se tornarem dados que permitam a identificação do titular por evolução tecnológica[506].

Não se encontra definição para a relação de "indissociavelmente ligação" entre dados pessoais e dados não pessoais. A solução proposta pelas Orientações da Comissão consiste em considerar que, nestas situações, a "separação dos dois tipos é impossível ou é

---

[504] «Dados pessoais», 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."

Também, *Considerando* (8) do RLFD.

[505] Nos termos do artigo 2.º, n.º 1 do RLFD:

"O presente regulamento aplica-se ao tratamento de dados eletrónicos que não sejam dados pessoais na União:

a) Prestado como um serviço a utilizadores residentes ou estabelecidos na União, independentemente de o prestador de serviços estar ou não estabelecido na União; ou

b) Realizado por uma pessoa singular ou coletiva com residência ou estabelecimento na União para as suas necessidades próprias."

[506] Artigo 2.º, n.º 2 do RLFD. Exemplificando casos de dados não pessoais e da sua utilidade económica e experimental, veja-se o Considerando (9): "A *internet* das coisas, a inteligência artificial e a aprendizagem automática, que estão em expansão, representam grandes fontes de dados não pessoais, por exemplo, em consequência da sua utilização em processos automatizados de produção industrial. Exemplos concretos de dados não pessoais incluem conjuntos de dados agregados e anonimizados utilizados para a análise de grandes volumes de dados, os dados relativos à agricultura de precisão que podem ajudar a controlar e a otimizar a utilização de pesticidas e de água ou ainda dados sobre as necessidades de manutenção de máquinas industriais. (...)".

considerada economicamente ineficiente ou tecnicamente inviável pelo responsável pelo tratamento"[507].

A notar que a definição de "tratamento", constante do artigo 3.º, n.º 2 do RLFD, tem uma proximidade relevante relativamente ao "tratamento de dados pessoais" (artigo 4.º, n.º 2 do *RGPD*), sendo, contudo, aplicável a dados não pessoais e a "conjuntos de dados".

A aplicação do conceito respeita às diversas operações que podem ser desenvolvidas com dados, independentemente da sua natureza.

Acompanhando as Orientações da Comissão, deve distinguir-se entre os dados não pessoais que podem ser classificados segundo a sua origem entre "desde o início", tratando-se aqui de informações insuscetíveis de revestir uma natureza pessoal[508] e "posteriormente anonimizados"[509].

As Orientações sublinham que é frequente que um conjunto de dados seja composto por dados pessoais e não pessoais[510].

Do ponto de vista da relação entre proteção de dados pessoais e regime aplicável a dados não pessoais o tema mais complexo consiste nas formas de proteção de dados anonimizados que, na sequência de "evolução tecnológica" se tornam "identificados ou identificáveis".

Assim, pensamos que, nos termos do *RGPD*, quando exista um tratamento de dados anonimizados – dados não pessoais – mas que perante a evolução tecnológica podem ser revertidos para dados pessoais permitindo a identificação dos respetivos titulares o artigo 35.º números 1 e 3, alínea a)[511].

---

[507] (COM (2019) 250), pp. 10/11.

[508] "Dados originalmente não relacionados com uma pessoa singular identificada ou identificável, tais como dados sobre as condições meteorológicas gerados por sensores instalados em turbinas eólicas ou dados sobre as necessidades de manutenção de máquinas industriais." p. 6.

[509] *Ibidem*.

[510] É avançada a designação de "conjunto misto de dados" (COM (2019) 250), p. 4.

[511] *Considerando* (84); "A fim de promover o cumprimento do presente regulamento nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos

Esta interpretação significa admitir que o *RGPD*, particularmente quanto às regras de *compliance* e segurança, é aplicável não apenas a dados pessoais existentes, mas a operações tecnológicas que possam vir a construir "novos" ou "de novo" dados pessoais, após a quebra da anonimização[512].

De acordo com o Grupo de Trabalho do artigo 29.º[513], apesar de não se fazer menção à transformação de dados não pessoais em dados pessoais, sustenta-se que o desenvolvimento tecnológico pode: "(...) envolver novas formas de recolha e utilização de dados, possivelmente com elevado risco para os direitos e as liberdades dos indivíduos. Na verdade, as consequências pessoais e sociais da implantação de uma nova tecnologia podem ser desconhecidas. Uma avaliação de impacto de proteção de dados [AIPD] ajudará o responsável pelo tratamento de dados a compreender e dar resposta a esses riscos. Por exemplo, algumas aplicações da «*Internet* das Coisas» podem ter um impacto significativo na vida quotidiana e na privacidade dos indivíduos e, como tal, exigem a realização de uma AIPD"[514].

Para assegurar que são cumpridas as regras do *RGPD*, podem ser invocados, por exemplo, a necessidade de cumprir as regras de proteção de dados desde a conceção e por defeito (artigo 25.º),

---

e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco.".

[512] Para além do artigo 35.º, importa analisar os *Considerandos* (89) e (91). De acordo com o primeiro: "(...) nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades. Os referidos tipos de operações de tratamento poderão, nomeadamente, envolver a utilização de novas tecnologias, ou pertencer a um novo tipo e não ter sido antecedidas por uma avaliação de impacto sobre a proteção de dados por parte do responsável pelo tratamento, ou ser consideradas necessárias à luz do período decorrido desde o tratamento inicial responsável pelo tratamento.".

[513] "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679." WP 248 rev.01, adotadas em 4 de abril de 2017. Revistas e adotadas pela última vez em 4 de outubro de 2017.

[514] *Idem*, p. 12

a prossecução das normas de segurança do tratamento de dados pessoais (artigo 32.º) e a aprovação de procedimento de certificação (artigo 42.º)[515].

1.2.2.1.2. A Diretiva de 2019 prevê a reutilização[516] de dados de empresas públicas[517], embora com algumas limitações (artigo 1.º, n.º 1, alínea b) e artigo 3.º, n.º 2)[518] , superando o regime da Diretiva de 2003[519].

De acordo com o artigo 1.º, n.º 2, alínea b), a Diretiva não é aplicável a dados de empresas públicas:

i) produzidos fora do âmbito da prestação de serviços de interesse geral, tal como definidos na lei ou em outras normas vinculativas do Estado-Membro;

---

[515] Manuel David Masseno, "Na Borda: Dados Pessoais e Não Pessoais nos dois Regulamentos da União Europeia" in *Disciplinarum Scientia.* Série: Sociais Aplicadas, Santa Maria, v. 16, n. 1, pp. 47-48. Disponível em : https://periodicos.ufn.edu.br/index.php/disciplinarumSA/article/view/3095.

[516] A definição prevista no artigo 2.º, n.º 11, identifica, essencialmente, as fontes da reutilização: "(...) a utilização por pessoas singulares ou coletivas de documentos na posse de: a) Organismos do setor público, para fins comerciais ou não comerciais que não correspondam ao objetivo inicial da missão de serviço público para o qual os documentos foram produzidos, excetuando o intercâmbio de documentos entre organismos do setor público exclusivamente no desempenho das suas missões de serviço público; ou b) Empresas públicas, para fins comerciais ou não comerciais que não correspondam ao objetivo inicial de prestação de serviços de interesse geral para os quais os documentos foram produzidos, excetuando o intercâmbio de documentos entre empresas públicas e organismos do setor público exclusivamente no desempenho das funções públicas dos organismos do setor público".

[517] Com definição prevista no artigo 2.º, n.º 3: "qualquer empresa ativa nos domínios estabelecidos no artigo 1.º, n.º 1, alínea b), em relação ao qual os organismos do setor público podem exercer, direta ou indiretamente, uma influência dominante, por motivos de direito de propriedade, participação financeira ou regras que lhe sejam aplicáveis. Presume-se a existência de influência dominante dos organismos do setor público sempre que estes organismos, de forma direta ou indireta:

a) Detenham a maioria do capital subscrito da empresa;

b) Disponham da maioria dos votos correspondentes às ações emitidas pela empresa;

c) Possam designar mais de metade dos membros do órgão administrativo, de direção ou de supervisão da empresa".

[518] O *Considerando* (26) transmite a natureza dos dados a colher nas empresas públicas: "A presente diretiva não contém qualquer obrigação geral de autorizar a reutilização de documentos produzidos por empresas públicas. A decisão de autorizar ou não a reutilização deverá caber às empresas públicas em causa, salvo disposição em contrário da presente diretiva, do direito nacional ou da União.".

[519] *Considerando* (24): "(...) a Diretiva 2003/98/CE aplica-se apenas a documentos na posse de organismos do setor público, excluindo as empresas públicas do seu âmbito de aplicação. Tal conduz a uma fraca

ii) relacionados com as atividades diretamente expostas à concorrência e, por conseguinte, nos termos do artigo 34.º da Diretiva 2014/25/UE[520], não sujeitas a regras de adjudicação de contratos.

Deve notar-se, porém, que, em conformidade com o *Considerando* (19) se apela a que os Estados-Membros permitam a reutilização de dados constantes de "(...) documentos na posse de empresas públicas relacionados com atividades que tenham sido consideradas, nos termos do artigo 34.º da Diretiva 2014/25/UE do Parlamento Europeu e do Conselho, diretamente expostas à concorrência."

Trata-se de ir além dos requisitos mínimos da Diretiva. No Direito português, de acordo com o artigo 20.º, alínea e) da LADA os documentos na posse de empresas públicas quando relacionados com atividades diretamente expostas à concorrência não podem ser objeto de reutilização[521].

1.2.2.3. A Diretiva de 2019, no seu artigo 12.º, estabelece uma regra de inexistência de acordos de exclusividade, para efeitos de reutilização de documentos (n.º 1).

No entanto, admite-se que podem verificar-se situações em que a prossecução do interesse público justifique acordos desta natureza, que devem ser revistos de três em três anos (n.º 2).

Para assegurar garantias de transparência, sempre que haja medidas que previsivelmente permitam uma limitação da disponibilidade para reutilização de documentos por parte de entidades que não

---

disponibilidade, para efeitos de reutilização, de documentos produzidos no âmbito da prestação de serviços de interesse geral em diversos domínios, nomeadamente no setor dos serviços de utilidade pública. Além disso, reduz consideravelmente o potencial para a criação de serviços transfronteiriços baseados em documentos na posse de empresas públicas que prestam serviços de interesse geral".

[520] Diretiva 2014/25/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014 relativa aos contratos públicos celebrados pelas entidades que operam nos setores da água, da energia, dos transportes e dos serviços postais e que revoga a Diretiva 2004/17/CE.

[521] Sobre reutilização na LADA ver Jorge Pação, "A reutilização da informação administrativa" in "*O Acesso à informação administrativa*", Tiago Fidalgo Freitas e Pedro Delgado Alves (org.), ICDP/ICJP, Almedina, 2021, pp. 341 e seguintes.

sejam o terceiro que participa no acordo, a sua publicação deve efetuar-se em linha. Os efeitos da disponibilidade dos dados destinados à reutilização devem ser objeto de exame periódico, devendo, em qualquer caso, ser revistos de três em três anos (n.º 4).

1.2.2.4. O Regulamento de execução 2023/138 da Comissão de 21 de dezembro de 2022[(522)], que estabelece uma lista de conjuntos específicos de dados de elevado valor e as disposições relativas à respetiva publicação e reutilização, tem na base o artigo 14.º da Diretiva de 2019 e o seu anexo I, que respeita a informações: a) geoespaciais; b) observação da Terra e do ambiente; c) meteorológicas; d) estatísticas; e) empresas e propriedade de empresas e f) mobilidade (n.º 1)[(523)].

Para garantir a reutilização de uma forma eficaz neste âmbito temático, o artigo 14.º, n.º 2 determina a disponibilização gratuita destes dados legíveis por máquina; acessíveis através de IPA; ou fornecidos sob a forma de descarregamento em bloco.

Esta disposição não se aplica a empresas públicas, se a disponibilização conduzisse a uma distorção da concorrência nos mercados relevantes (n.º 3), a bibliotecas (n.º 4) e quando os organismos públicos sejam obrigados a cobrir os seus custos e não se encontrem isentos dessa função (n.º 5).

A publicação e reutilização dos conjuntos de dados de elevado valor são compatíveis com a emissão de licenças-tipo abertas digitais (n.º 1)[(524)].

---

(522) O Regulamento encontra-se em vigor, apesar de ainda não produzir efeitos (artigo 6.º).

(523) Deve notar-se que o Regulamento de execução faz menção expressa à da Diretiva 2007/2/CE relativa a dados de categorias geoespacial, meteorológica e de observação da Terra e do ambiente e à Diretiva 2005/44/CE relativa a dados de mobilidade (artigo 2.º, números 2 e 3).

(524) Importa verificar o Considerando (12) do Regulamento de execução: "A Diretiva (UE) 2019/1024 tem como objetivo promover a utilização de licenças públicas normalizadas disponíveis em linha para a reutilização de informações do setor público. As Orientações da Comissão sobre as licenças-tipo recomendadas, os conjuntos de dados e a cobrança de encargos pela reutilização de documentos «Comunicação da Comissão: Orientações sobre as licenças-tipo recomendadas, os conjuntos de dados e a cobrança de encargos pela reutilização de documentos (2014/C 240/01) in JO C 240 de 24.7.2014, p. 1»

Com este regime pretende-se que a lista de conjuntos de dados de elevado valor e com "maior potencial socioeconómico sejam disponibilizados para reutilização com um mínimo de restrições legais e técnicas e de forma gratuita"[525].

Em sede de proteção de dados pessoais, O Regulamento de execução não contém referências no articulado, dedicando-lhe, porém, o *Considerando* (8).

Aí se refere que a disponibilização de conjuntos de dados de elevado valor para reutilização que implique o tratamento de dados pessoais deve ser realizado em conformidade com o *RGPD*. A notar que não existe, contudo, menções às fontes de legitimidade previstas no artigo 6.º do *RGPD*. Assim, a legislação europeia não assegura a necessidade do consentimento do titular dos dados para a realização destes tratamentos, abrindo a possibilidade para, por exemplo, fundamentos de legitimidade baseados na legislação ou no interesse público.

Relativamente às metodologias a utilizar – associadas a medidas de segurança – menciona-se que: "Os Estados-Membros devem utilizar métodos e técnicas adequadas (como a generalização, a agregação, a supressão, a anonimização, a privacidade diferencial ou a aleatorização), disponibilizando assim a maior quantidade possível de dados para reutilização".

identificam as licenças «Creative Commons» (CC) como um exemplo de licenças públicas normalizadas recomendadas. As licenças CC são desenvolvidas por uma organização sem fins lucrativos e tornaram-se uma das principais soluções de licenciamento para informações do setor público, resultados de investigação e material do domínio cultural em todo o mundo. Por conseguinte, é necessário que o presente regulamento de execução remeta para a versão mais recente do conjunto de licenças CC, a saber, CC 4.0. Uma licença equivalente ao conjunto de licenças CC pode prever disposições adicionais, como a obrigação de o reutilizador incluir atualizações fornecidas pelo detentor dos dados e de especificar quando os dados foram atualizados pela última vez, desde que não restrinjam as possibilidades de reutilização dos dados.".

(525) *Considerando* (2) do Regulamento de execução de 2023.

Com idêntico propósito, o *Considerando* (3) alude aos princípios FAIR: "a disponibilização de conjuntos de dados de elevado valor em condições ideais permite reforçar as políticas de livre acesso aos dados nos Estados-Membros, com base nos princípios de facilidade de localização, acessibilidade, interoperabilidade e reutilização (princípios FAIR)".

De acordo com o *Considerando* (7) do Regulamento de execução, o seu âmbito de aplicação não inclui os dados na posse de empresas públicas.

1.2.3. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Uma estratégia europeia para os dados (COM (2020) 66 final, Bruxelas, 19 .2.2020)[526].

A definição da estratégia a que alude a Comunicação de 2020 baseia-se na exploração máxima de uma economia assente em dados, conduzindo a UE a modelos de desenvolvimento e liderança que permitam o progresso científico económico e social fundado no conhecimento proveniente de informação, especialmente de caráter público, já existente no mercado único: "o objetivo é criar um espaço único europeu de dados – um verdadeiro mercado único de dados, aberto a dados de todo o mundo – em que os dados pessoais e não pessoais, incluindo dados comerciais sensíveis, estejam seguros e as empresas tenham fácil acesso (...)"[527].

Neste contexto, a UE deve "melhorar as suas estruturas de governação para manuseamento de dados e de aumentar os repositórios de dados de qualidade disponíveis para utilização e reutilização"[528].

A Comunicação ressalta que a economia assente em dados permite uma "réplica praticamente a custo zero"[529] ao mesmo tempo que favorece a utilização por várias pessoas e entidades do mesmo bem.

Os propósitos assim definidos carecem de legislação adequada que regule, nomeadamente: o regime relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à

[526] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52020DC0066.

[527] COM (2020) 66 final, p. 4.

[528] *Idem*, p. 1.

[529] *Idem*, p. 4.

livre circulação desses dados (Regulamento 2016/679); o livre fluxo de dados não pessoais na União Europeia (Regulamento 2018/1807); os dados abertos, como temos observado na Diretiva 2019/1024 de 20 de junho e no Regulamento de execução 2023/138 da Comissão; a governação europeia de dados (Regulamento 2022/868), os serviços digitais (Regulamento 2022/2065) e a matéria da cibersegurança (Regulamento 2019/88).

Na relação com matéria de proteção de dados, a Comunicação refere a necessidade utilizar as melhores praticas no que respeita à segurança da informação como é o caso, por exemplo, da pseudonimização[530].

Relativamente ao controlo e acesso por parte dos titulares de dados sobre informação a si respeitante, a Comunicação enfatiza o direito à portabilidade de dados pessoais (artigo 20.º do *RGPD*) nos "espaços de dados pessoais", assim se garantindo um controlo mais eficaz por parte do titular dos dados pessoais relativamente à informação gerada automaticamente[531].

De forma mais detalhada, a Comunicação apela à relação entre a utilização e a reutilização dos dados de saúde para fins de evolução científica, desde que os titulares dos dados tenham direito a aceder e controlar os seus dados e de solicitar a sua portabilidade[532].

Estabelecendo a relação entre a utilização e reutilização de dados pessoais e as fontes de legitimidade previstas no *RGPD*, a Comissão faz notar que: "os titulares dos dados precisam de estar seguros de que, após terem dado consentimento para que os seus dados sejam partilhados, os sistemas de saúde os utilizam de forma ética e garantem que o consentimento pode ser retirado a qualquer momento"[533].

---

[530] *Idem*, p. 16.

[531] *Idem*, p. 20.

A Comunicação estabelece, também, o direito à portabilidade em referência feita a "intermediários neutros", numa alusão à proposta que veio a ser aprovada com o Regulamento 2022/868. Ibidem.

[532] *Idem*, p. 29.

[533] *Ibidem*.

Esta Comunicação frisa a necessidade de recolher informação pública em regime de dados abertos para treinar sistemas de inteligência artificial, que permita o "reconhecimento de padrões e do estabelecimento de novas correlações para técnicas de previsão mais sofisticadas conducentes a melhores decisões"[534-535].

2. O Regulamento 2022/868[536], dos instrumentos em vigor, é o último a tratar, com densidade, a partilha e reutilização de dados por entidades públicas. É aplicável desde 24 de setembro de 2023 (artigo 38.º). O Regulamento de 2022 não prejudica a aplicação de outros instrumentos jurídicos que rejam "(...) matéria de acesso e utilização dos dados para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, nem de cooperação internacional nesse contexto"[537].

O Regulamento não prejudica a aplicação do direito da concorrência (artigo 1.º, n.º 4)[538], não afetando também atividades relacionadas com a segurança pública, a defesa e a segurança nacional (artigo 1.º, n.º 5)[539].

---

[534] *Idem*, p. 3.

[535] A "vertente experimental" acompanha, em diversos passos a Comunicação: "Uma vez que é difícil compreender plenamente todos os elementos desta transição para uma economia ágil dos dados, a Comissão abstém-se deliberadamente de adotar regulamentação ex ante excessivamente pormenorizada e prescritiva, preferindo uma abordagem flexível da governação que favoreça a experimentação." *Idem*, p. 12.

Ver: Patrícia Carneiro, "Regulamento Geral sobre a Proteção de Dados e o mercado de dados – Mercado de dados 1.0 e a licitude da partilha de dados (pessoais) através de serviços de intermediação de dados no âmbito do Regulamento de Governação de Dados, por via do consentimento do titular dos dados – uma imposição de base legal?" in *"Anuário de Proteção de Dados"*, 2023, Coordenação Francisco Pereira Coutinho e Graça Canto Moniz, Universidade Nova de Lisboa. Faculdade de Direito. CEDIS, p. 156.

[536] Para uma apreciação crítica à proposta deste Regulamento, ver: "EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). Disponível em: https://edpb.europa.eu/our-work-tools/our documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en.

[537] *Considerando* (3). Também, artigo 1.º, n.º 2.

[538] *Considerando* (13): "Os organismos do setor público deverão respeitar o direito da concorrência ao estabelecerem os princípios de reutilização dos dados que detêm, evitando celebrar acordos que possam ter por objetivo ou efeito a criação de direitos exclusivos de reutilização de certos dados.".

[539] Ver: *Considerando* (3).

O âmbito de aplicação do Regulamento, de acordo com o artigo 1.º, n.º 1, respeita ao seguinte:

(i) Determinação das condições para a reutilização de determinadas categorias de dados detidos por organismos do setor público;

(ii) Definição de um regime de notificação e supervisão para a prestação de serviços de intermediação de dados;

(iii) Determinação de um regime para o registo voluntário das entidades que recolhem e tratam dados disponibilizados para fins altruístas;

(iv) Estabelecer um regime para a criação de um Comité Europeu da Inovação de Dados.

2.1. No que respeita a novas normas sobre a reutilização[540], o artigo 3.º, n.º 1 do Regulamento prevê que este é aplicável a informações sobre:[541]

(i) Confidencialidade comercial, nomeadamente segredos comerciais, profissionais e empresariais;

(ii) Confidencialidade estatística;

(iii) Proteção dos direitos de propriedade intelectual de terceiros; ou Proteção dos dados pessoais, na medida em que os dados em causa

---

[540] Para efeitos deste Regulamento, reutilização está definido como "a utilização, por pessoas singulares ou coletivas, de dados detidos por organismos do setor público, realizada para fins comerciais ou não comerciais que não correspondem à finalidade inicial da missão de serviço público para a qual os dados foram produzidos, excetuando o intercâmbio de dados entre organismos do setor público exclusivamente no desempenho das suas missões de serviço público (artigo 2.º, n.º 2).".

[541] "(...) A Diretiva (UE) 2019/1024 e o direito setorial da União garantem que os organismos do setor público tornem um maior número dos dados que produzem facilmente disponível para utilização e reutilização. No entanto, determinadas categorias de dados, como os dados comerciais confidenciais, os dados que estão sujeitos a confidencialidade estatística e os dados protegidos por direitos de propriedade intelectual de terceiros, incluindo segredos comerciais e dados pessoais, que se encontram em bases de dados públicas, muitas vezes não são disponibilizados, nem sequer para atividades de investigação ou de inovação de interesse público, apesar dessa disponibilidade ser possível nos termos do direito da União aplicável, em particular do Regulamento (UE) 2016/679 e das Diretivas 2002/58/CE e (UE) 2016/680. Devido à sensibilidade desses dados, a sua disponibilização exige o respeito prévio de certos requisitos processuais técnicos e jurídicos, principalmente para garantir o respeito dos direitos de terceiros sobre os dados em questão ou limitar o impacto negativo nos direitos fundamentais, no princípio da não discriminação e na proteção de dados.".

não sejam abrangidos pelo âmbito de aplicação da Diretiva (UE) 2019/1024.

No que respeita aos casos de confidencialidade comercial, nomeadamente segredos comerciais, profissionais e empresariais, importa analisar o Considerando (10)[542], bem como o artigo 5.º, n.º 5:

"A menos que o direito nacional preveja salvaguardas específicas sobre as obrigações de confidencialidade aplicáveis relacionadas com a reutilização de dados referidos no artigo 3.º, n.º 1, o organismo do setor público subordina a utilização dos dados fornecidos nos termos do n.º 3 do presente artigo ao cumprimento, por parte do reutilizador, de uma obrigação de confidencialidade que proíba a divulgação de qualquer informação que comprometa os direitos e interesses de terceiros e que o reutilizador possa ter adquirido apesar das salvaguardas instituídas. Os reutilizadores ficam proibidos de reidentificar qualquer titular dos dados a quem os dados digam respeito e devem tomar medidas técnicas e operacionais para prevenir a reidentificação e para notificar ao organismo do setor público qualquer violação de dados que resulte na reidentificação dos titulares dos dados em causa. Em caso de reutilização não autorizada de dados não pessoais, o reutilizador informa, sem demora, se for caso disso com a assistência do organismo do setor público, as pessoas coletivas cujos direitos e interesses possam ser afetados".

(542) "As categorias de dados detidos por organismos do setor público cuja reutilização deverá ser regida pelo presente regulamento não são abrangidas pelo âmbito de aplicação da Diretiva (UE) 2019/1024, que exclui os dados que não são acessíveis por motivos de confidencialidade comercial ou estatística e os dados incluídos em obras ou noutro material protegido relativamente aos quais terceiros têm direitos de propriedade intelectual. Os dados comerciais confidenciais incluem os dados protegidos por segredos comerciais, o saber-fazer protegido e quaisquer outras informações cuja divulgação indevida possa ter um impacto na posição de mercado ou na saúde financeira da empresa. O presente regulamento deverá aplicar-se aos dados pessoais que não são abrangidos pelo âmbito de aplicação da Diretiva (UE) 2019/1024 na medida em que o regime de acesso exclui ou restringe o acesso a esses dados por razões de proteção de dados, privacidade e integridade da pessoa em causa, nomeadamente em conformidade com as regras em matéria de proteção de dados. A reutilização de dados que possam conter segredos comerciais deverá ter lugar sem prejuízo do disposto na Diretiva (UE) 2016/943, que estabelece o quadro para a aquisição, utilização ou divulgação legais de segredos comerciais.".

A aplicação do Regulamento às categorias de dados previstas no artigo 3.º, n.º 1 deve ser, assim, organizada:

(i) A concessão ou a recusa de acesso à reutilização de dados depende da comunicação pública a efetuar por organismos públicos que identificam pontos de identificação únicos[543] (artigo 8.º), assistidos pelos organismos competentes a que se refere o artigo 7.º, n.º 1;

(ii) "(...) O ponto de informação único é competente para receber os pedidos de informação ou os pedidos de reutilização das categorias de dados referidas no artigo 3.º, n.º 1, e transmite-os, sempre que possível e adequado por meios automatizados, aos organismos do setor público competentes (...)" (artigo 8.º, n.º 2);

(iii) O acesso e reutilização remotos dos dados devem realizar-se num ambiente de tratamento seguro disponibilizado ou controlado pelo organismo do setor público (artigo 5.º, n.º 2, alínea b)[544];

(iv) Sempre que os pedidos de reutilização puserem em causa a legislação sobre proteção de dados, particularmente o *RGPD*, os organismos públicos devem garantir que os "requisitos para a realização de uma avaliação de impacto em matéria de proteção de dados e a consulta da autoridade de controlo, nos termos dos artigos 35.º e 36.º do *RGPD* e os riscos para os direitos e interesses dos titulares dos dados tenham sido considerados mínimos, poderá ser permitida a reutilização dos dados nas instalações ou de forma remota num ambiente de tratamento seguro."[545].

---

[543] *Considerando* (26): "(...) O ponto de informação único deverá dispor de uma lista de recursos com todos os recursos de dados disponíveis, incluindo, se for caso disso, os recursos de dados disponíveis nos pontos de informação setoriais, regionais ou locais, com informações relevantes que descrevam os dados disponíveis (...)".

[544] "«Ambiente de tratamento seguro» (artigo 2.º, n.º 20), o ambiente físico ou virtual e os meios organizacionais destinados a assegurar o cumprimento do direito da União, tal como o Regulamento (UE) 2016/679, em especial no que respeita aos direitos dos titulares dos dados, os direitos de propriedade intelectual, a confidencialidade comercial e estatística, a integridade e a acessibilidade, bem como o cumprimento do direito nacional aplicável e permitir à entidade que fornece o ambiente de tratamento seguro determinar e supervisionar todas as ações de tratamento de dados, incluindo visualização, o armazenamento, o descarregamento e a exportação de dados, bem como o cálculo de dados derivados através de algoritmos computacionais.".

[545] *Considerando* (15).

2.2. De acordo com o artigo 2.º, n.º11 o Regulamento estabelece a definição de «Serviço de intermediação de dados»: "um serviço que visa estabelecer relações comerciais para efeitos de partilha de dados[546] entre um número indeterminado de titulares dos dados e detentores dos dados[547], por um lado, e utilizadores de dados[548], por outro, através de meios técnicos, jurídicos ou outros, inclusive para o exercício dos direitos dos titulares dos dados em relação aos dados pessoais, excluindo, pelo menos, o seguinte:

(a) Serviços que obtêm dados junto dos detentores dos dados e agregam, enriquecem ou transformam os dados obtidos com o objetivo de lhes acrescentar um valor substancial e licenciam a utilização dos dados resultantes aos utilizadores de dados, sem estabelecer uma relação comercial entre os detentores dos dados e os utilizadores dos dados;

b) Serviços centrados na intermediação de conteúdos protegidos por direitos de autor;

c) Serviços exclusivamente utilizados por um único detentor dos dados para permitir a utilização dos dados detidos por esse detentor dos dados, ou utilizados por várias pessoas coletivas no seio de um grupo fechado, inclusive no âmbito de relações com fornecedores ou clientes ou colaborações contratualmente estabelecidas, em especial os que tenham como principal objetivo assegurar funcionalidades de objetos e dispositivos ligados à Internet das coisas;

---

[546] Artigo 2.º, n.º 10: "«Partilha de dados», o fornecimento de dados, por um titular dos dados ou um detentor dos dados, a um utilizador de dados para fins da utilização conjunta ou individual dos dados em causa, com base em acordos voluntários ou no direito da União ou nacional, diretamente ou através de um intermediário, por exemplo, ao abrigo de licenças abertas ou comerciais sujeitas a uma taxa ou gratuitas.".

[547] Artigo 2.º, n.º 8: "«Detentor dos dados», uma pessoa coletiva, incluindo organismos do setor público e organizações internacionais, ou uma pessoa singular que não seja o titular dos dados no que diz respeito aos dados específicos em causa, que, em conformidade com o direito da União ou o direito nacional aplicáveis, tem o direito de conceder acesso a determinados dados pessoais ou dados não pessoais ou de os partilhar.".

[548] Artigo 2.º, n.º 9: "«Utilizador dos dados», uma pessoa singular ou coletiva que tem acesso legal a determinados dados pessoais ou não pessoais e que tem direito, inclusive ao abrigo do *RGPD* no que respeita aos dados pessoais, a utilizá-los para fins comerciais ou não comerciais".

d) Serviços de partilha de dados oferecidos por organismos do setor público que não visam estabelecer relações comerciais.

Os "serviços de intermediação de dados" encontram-se explicados no *Considerando* (33). De modo a garantir que não existe utilização indevida ou afastada do princípio da finalidade, "é necessário que os prestadores de serviços de intermediação de dados atuem apenas como intermediários nas transações e não utilizem os dados trocados para qualquer outro fim"[549].

O Regulamento exige, também, uma separação entre o serviço de intermediação de dados e quaisquer outros serviços prestados, a fim de evitar conflitos de interesses.

Assim, o serviço de intermediação de dados deverá ser prestado através de uma pessoa coletiva distinta das outras atividades desse prestador de serviços de intermediação de dados[550].

De acordo com o artigo 12.º, sublinhamos que:

i) Os serviços de intermediação de dados podem incluir a oferta, aos detentores dos dados ou aos titulares dos dados, de instrumentos e serviços específicos adicionais que visem especificamente facilitar o intercâmbio de dados, tais como o armazenamento temporário, a curadoria, a conversão, a anonimização e a pseudonimização; os instrumentos e serviços em causa só podem ser utilizados mediante pedido ou aprovação expressos do detentor dos dados ou do titular dos dados, e os instrumentos de terceiros disponibilizados nesse contexto não podem utilizar os dados para outros fins (alínea e);

(ii) O prestador de serviços de intermediação de dados deve dispor de procedimentos para prevenir práticas fraudulentas ou abusivas de partes que procurem ter acesso através do seu serviço de intermediação de dados (alínea g);

---

[549] *Considerando* (33).

[550] *Ibidem*.

(**iii**) O prestador de serviços de intermediação de dados deve tomar as medidas adequadas para assegurar a interoperabilidade com outros serviços de intermediação de dados, nomeadamente através de normas abertas de uso corrente no setor em que os prestadores de serviços de intermediação de dados operam (alínea i);

(**iv**) O prestador de serviços de intermediação de dados deve tomar as medidas necessárias para garantir um nível de segurança adequado do armazenamento, do tratamento e da transmissão de dados não pessoais, devendo ainda garantir o mais elevado nível de segurança possível do armazenamento e da transmissão de informações sensíveis do ponto de vista da concorrência (alínea l); (v) O prestador de serviços de intermediação de dados que oferece serviços a titulares dos dados deve agir no melhor interesse destes ao facilitar o exercício dos seus direitos, em especial informando-os e, se for caso disso, aconselhando-os de forma concisa, transparente, inteligível e facilmente acessível sobre as utilizações previstas dos dados por parte dos utilizadores dos dados e sobre as condições gerais associadas a essas utilizações, antes de os titulares dos dados darem o seu consentimento (alínea m);

(**vi**) Caso um prestador de serviços de intermediação de dados faculte instrumentos para obter o consentimento dos titulares dos dados ou a autorização para o tratamento dos dados disponibilizados pelos detentores dos dados, deve, se for caso disso, especificar a jurisdição de país terceiro em que a utilização dos dados se destina a ser efetuada e facultar aos titulares dos dados instrumentos para dar e retirar o consentimento, e aos detentores dos dados instrumentos para dar e retirar a autorização para o tratamento de dados (alínea n).

Entendemos que as referências episódicas ao consentimento feitas no Regulamento de 2022, não podem justificar que todos os processos de reutilização o tenham como fundamento de licitude. O Regulamento prevê a necessidade de cumprimento do *RGPD*, que passa pela determinação de

um fundamento de legitimidade (essencialmente artigo 6.º do *RGPD*), não impondo o consentimento como fundamento único[551].

2.3. O artigo 2.º, n.º 16 prevê a definição de «Altruísmo de dados»: "a partilha voluntária de dados, com base no consentimento dos titulares dos dados para o tratamento dos respetivos dados pessoais ou na autorização, por parte de outros detentores dos dados, da utilização dos seus dados não pessoais, sem que esses titulares ou detentores procurem ou recebam uma gratificação que vá além de uma compensação pelos custos em que incorrem ao disponibilizarem os seus dados, para fins de interesse geral, previstos no direito nacional, se aplicável, tais como os cuidados de saúde[552], a luta contra as alterações climáticas, a melhoria da mobilidade, a facilitação do desenvolvimento, produção e divulgação de estatísticas oficiais, a melhoria da prestação dos serviços públicos, a elaboração de políticas públicas ou a investigação científica de interesse geral"[553].

O artigo 16.º prevê que os Estados-Membros podem dispor de mecanismos organizacionais ou técnicos, ou ambos, para facilitar o altruísmo de dados.

A criação de registos públicos de organizações de altruísmo de dados reconhecidas (artigo 17.º) é atualizada regularmente (n.º 1). O artigo 18.º prevê os elementos que devem constar de organizações de altruísmo.

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

---

[553] Deve notar-se que: "As organizações de altruísmo de dados reguladas pelo presente regulamento não deverão ser consideradas prestadores de serviços de intermediação de dados, desde que esses serviços não estabeleçam uma relação comercial entre os potenciais utilizadores de dados, por um lado, e os titulares dos dados e os detentores dos dados que disponibilizam os dados por fins altruístas, por outro. Não deverão ser considerados serviços de intermediação de dados na aceção do presente regulamento outros serviços que não visem estabelecer relações comerciais, como os repositórios destinados a permitir a reutilização de dados de investigação científica em conformidade com os princípios do acesso aberto."

O citado Regulamento já se encontra em vigor, mas produzirá efeitos apenas a partir de 12 de setembro de 2025 (artigo 50.º)[554].

O seu conteúdo afasta-se do Regulamento de 2019 e do Regulamento de 2022, limitando a reutilização de dados, em detrimento dos mecanismos aí previstos[555].

Quanto ao conteúdo do Regulamento de 2023, revela o *Considerando* (5):

"O presente regulamento garante que os utilizadores de um produto conectado ou serviço conexo[556] na União podem aceder, em tempo útil, aos dados gerados pela utilização desse produto ou serviço conexo, e que podem utilizar esses dados, nomeadamente partilhando-os com terceiros da sua escolha. Impõe aos detentores dos dados a obrigação de disponibilizarem dados aos utilizadores e a terceiros escolhidos pelo utilizador em determinadas circunstâncias.

---

[554] Outras regras relativas à aplicabilidade do Regulamento constam, também, do artigo 50.º: "A obrigação decorrente do artigo 3.º, n.º 1, é aplicável aos produtos conectados e serviços com eles relacionados colocados no mercado após 12 de setembro de 2026.

O capítulo III é aplicável às obrigações de disponibilização de dados nos termos de disposições do direito da União ou da legislação nacional adotada em conformidade com o direito da União que entrem em vigor após 12 de setembro de 2025.

O capítulo IV é aplicável aos contratos celebrados após 12 de setembro de 2025.

O capítulo IV é aplicável a partir de 12 de setembro de 2027 aos contratos celebrados em 12 de setembro de 2025, ou antes dessa data, desde que:

a) Sejam de duração indeterminada; ou

b) Expirem pelo menos 10 anos a contar de 11 de janeiro de 2024.".

[555] *Considerando* (70): "O objetivo da obrigação de fornecer os dados consiste em assegurar que os organismos do setor público, a Comissão, o Banco Central Europeu ou os órgãos da União dispõem dos conhecimentos necessários para responder, prevenir ou recuperar de emergências públicas ou para manter a capacidade de desempenhar funções específicas expressamente previstas por lei. Os dados obtidos por essas entidades poderão ser comercialmente sensíveis. Por conseguinte, nem o Regulamento (UE) 2022/868 nem a Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho deverão ser aplicáveis aos dados disponibilizados nos termos do presente regulamento, nem estes deverão ser considerados como dados abertos disponíveis para reutilização por terceiros. Todavia, isso não deverá afetar a aplicabilidade da Diretiva (UE) 2019/1024 à reutilização de estatísticas oficiais para cuja elaboração tenham sido utilizados dados obtidos nos termos do presente regulamento, desde que a reutilização não inclua os dados subjacentes.".

[556] Artigo 2.º, n.º 6 "«Serviço conexo», um serviço digital, que não seja um serviço de comunicações eletrónicas, incluindo software, conectado ao produto no momento da aquisição ou locação de tal modo que a sua ausência impediria que o produto conectado desempenhasse uma ou mais das suas funções, ou conectado posteriormente ao produto pelo fabricante ou por terceiros, a fim de aumentar, atualizar ou adaptar as funções do produto conectado".

Garante também que os detentores dos dados disponibilizam os dados aos destinatários dos dados na União ao abrigo de cláusulas e condições equitativas, razoáveis e não discriminatórias e de forma transparente. As regras do direito privado são fundamentais no regime global da partilha de dados.

Por conseguinte, o presente regulamento adapta as regras do direito contratual e impede a exploração dos desequilíbrios contratuais que dificultam o acesso equitativo aos dados e a sua utilização. O presente regulamento garante também que, em caso de necessidade excecional, os detentores dos dados disponibilizam aos organismos do setor público, à Comissão, ao Banco Central Europeu ou aos órgãos da União os dados necessários para o desempenho de uma função específica de interesse público. Além disso, visa facilitar a mudança entre serviços de tratamento de dados e reforçar a interoperabilidade dos dados e dos mecanismos e serviços de partilha de dados na União. O presente regulamento não deverá ser interpretado como reconhecendo ou como conferindo aos detentores dos dados qualquer novo direito de utilizar os dados gerados pela utilização de um produto conectado ou serviço conexo".

A proteção de dados pessoais no Regulamento de 2023 é mencionada de forma acentuada no *Considerando* (7): "(...) O presente regulamento complementa e não prejudica o direito da União em matéria de proteção de dados pessoais e privacidade, nomeadamente os Regulamentos (UE) 2016/679 e (UE) 2018/1725 e a Diretiva 2002/58/CE. Nenhuma disposição do presente regulamento deverá ser aplicada ou interpretada de forma a diminuir ou limitar o direito à proteção dos dados pessoais ou o direito à privacidade e à confidencialidade das comunicações. Qualquer tratamento de dados pessoais nos termos do presente regulamento deverá cumprir o direito da União em matéria de proteção de dados, incluindo o requisito de que haja um fundamento jurídico válido para o tratamento nos termos do artigo 6.º do Regulamento (UE) 2016/679 (...)."

De acordo com o *Considerando* (6): "A geração de dados é o resultado das ações de, pelo menos, dois intervenientes, nomeadamente o projetista ou o fabricante de um produto conectado, que, em muitos casos, pode ser também um prestador de serviços conexos, e o utilizador do produto conectado ou serviço conexo. Suscita questões de equidade na economia digital, uma vez que os dados registados por produtos conectados ou serviços conexos constituem um contributo importante para os serviços pós-venda, complementares e outros (...)."

Referências

Jorge Pação, "A reutilização da informação administrativa" in "O Acesso à informação administrativa", Tiago Fidalgo Freitas e Pedro Delgado Alves (org.), ICDP/ICJP, Almedina, 2021;

Manuel David Masseno, "Na Borda: Dados Pessoais e Não Pessoais nos dois Regulamentos da União Europeia" in *Disciplinarum Scientia.* Série: Sociais Aplicadas, Santa Maria, v. 16, n. 1, pp. 47-48. Disponível em: https://periodicos.ufn.edu.br/index.php/disciplinarum-SA/article/view/3095;

Nuno Xavier e Gabriel Osório de Barros, "Em análise dados abertos em Portugal", Gabinete de Estratégia e Estudos, data 21-11-2022, disponível em: https://www.gee.gov.pt/pt/estudos--e-seminarios/artigos-category/32493-em-analise-dados-abertos-em-portugal?highlight=WyJkYWRvcyIsImFiZXJ0b3MiLCJkYWRvcyBhYmVydG9zIl0;

Patrícia Carneiro, "Regulamento Geral sobre a Proteção de Dados e o mercado de dados – Mercado de dados 1.0 e a licitude da partilha de dados (pessoais) através de serviços de intermediação de dados no âmbito do Regulamento de Governação de Dados, por via do consentimento do titular dos dados – uma imposição de base legal?" in "Anuário de Proteção de Dados", 2023, Coordenação Francisco Pereira Coutinho e Graça Canto Moniz, Universidade Nova de Lisboa. Faculdade de Direito. CEDIS;

Tiago Branco da Costa, "O Altruismo (Económico?) de dados: Breves Considerações sobre o Espaço Europeu de dados de saúde e a proteção de dados pessoais" in "Liber Amicorum Benedita Mc Crorie", Volume II, Universidade do Minho, in: https://doi.org/10.21814/uminho.ed.105.30;

Parecer n.º 3/99, sobre preservação de dados de tráfico de ISPs para finalidades de law enforcement: Grupo de Trabalho do artigo 29.º, 5085/99/EN/FINAL WP 25, 7 de setembro de 1999;

Parecer n.º 5/2001, sobre o Relatório Especial do Provedor de Justiça Europeu ao Parlamento Europeu na sequência do projeto de recomendação à Comissão Europeia relativo à reclamação 713/98/IJH: Grupo de Trabalho do artigo 29.º, 5003/00/EN/Final WP 44, 17 de maio de 2001;

Parecer n.º 7/2003, sobre a reutilização da informação do sector público e proteção dos dados pessoais – Estabelecer um equilíbrio: Grupo de Trabalho do artigo 29.º, 10936/03/PT WP 83, 12 de dezembro de 2003;

Comunicação da Comissão ao Parlamento Europeu e ao Conselho: Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados (COM (2019) 250, de 29.05.2019);

EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). Disponível em: https://edpb.europa.eu/our-work-tools/ourdocuments/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en;

Diretiva do Conselho 90/313/CEE, de 7 de junho de 1990, relativa à liberdade de acesso à informação em matéria de ambiente;

Diretiva 2003/98/CE do Parlamento Europeu e do Conselho, de 17 de novembro de 2003 relativa à reutilização de informações do sector público;

Diretiva 2013/37/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, que altera a Diretiva 2003/98/CE relativa à reutilização de informações do setor público;

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;

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

Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia;

Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho, de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados);

Regulamento de execução 2023/138 da Comissão, de 21 de dezembro de 2022, que estabelece uma lista de conjuntos específicos de dados de elevado valor e as disposições relativas à respetiva publicação e reutilização;

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

Lei n.º 26/2016, de 22 de agosto, Lei de Acesso aos Documentos Administrativos – (LADA);

Lei n.º 68/2021, de 26 de agosto, Aprova os princípios gerais em matéria de dados abertos e transpõe para a ordem jurídica interna a Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informação do setor público, alterando a Lei n.º 26/2016, de 22 de agosto;

Declaração de Retificação n.º 31/2021, de 20 de setembro, publicado no DRE (Série I), de 26 de agosto de 2021;

Resolução do Conselho de Ministros n.º 131/2021, de 10 de setembro, sobre a "Estratégia para a Transformação Digital da Administração Pública 2021-2026.

12 | INTELIGÊNCIA ARTIFICIAL, PROTEÇÃO DE DADOS SENSÍVEIS E A VULNERABILIDADE HUMANA: O PLANO LEGAL E O PLANO DA BIOÉTICA

*Cristina Caldeira**

Resumo

O estudo centra-se numa reflexão sobre a transformação digital da sociedade e os debates ocorridos, sobretudo em 2023, em torno do impacto da aplicação da inteligência artificial (IA) em especial na área da saúde. Trata-se de uma tecnologia emergente, caracterizada pela polivalência, que alcançou maior visibilidade a partir de 2016, numa altura em que a União Europeia desenhava a sua estratégia sobre a IA, a que se seguiu um pacote legislativo em torno da proteção de dados pessoais (*RGPD*), o qual consagra um regime reforçado de proteção ao tratamento de dados sensíveis. Posteriormente foi criado o *Artificial Intelligence Act*, um quadro regulamentar baseado no risco e publicadas as regras aplicadas à responsabilidade civil extracontratual à inteligência artificial, bem como o Regulamento relativo à Governação Europeia dos Dados. Em ordem ao título: *Inteligência Artificial, Proteção de Dados Sensíveis e a Vulnerabilidade Humana: o plano legal e o plano da bioética* elencamos os seguintes pontos: Sistemas de IA baseados nos valores da União; Transformação dos municípios através da aplicação da IA na área da saúde; Regras específicas relativas aos sistemas de IA aplicados à área da saúde; Privacidade e confidencialidade dos dados sensíveis em contexto multinível; Princípios éticos aplicáveis à prática clínica e investigação médica; Integridade da investigação versus confidencialidade da informação clínica; Bioética e o princípio da autonomia: o consentimento informado; Vulnerabilidade como um conceito ético-jurídico e Governação Europeia de Dados.

Palavras-chave: Dignidade humana, inteligência artificial, dados relativos à saúde, privacidade, proteção de dados sensíveis, vulnerabilidade, bioética.

* Professora Auxiliar da Universidade Europeia, Investigadora FCT.I.P., Bolseira da Fundação Gulbenkian na Universidade de Oxford, St Antony's College.

Introdução

A intensificação dos debates em torno dos impactos da inteligência artificial (IA) e a discriminação algorítmica, marcaram o ano de 2023. Na mensagem do Dia Mundial da Paz, a 1 de janeiro de 2024, o Santo Padre Francisco realça que,

> "Os progressos da informática e o desenvolvimento das tecnologias digitais, nas últimas décadas, começaram já a produzir profundas transformações na sociedade global e nas suas dinâmicas. Os novos instrumentos digitais estão a mudar a fisionomia das comunicações, da administração pública, da instrução, do consumo, dos intercâmbios pessoais e de inúmeros outros aspetos da vida diária. Além disso as tecnologias que se servem duma multiplicidade de algoritmos podem, dos vestígios digitais deixados na *internet*, extrair dados que permitem controlar os hábitos mentais e relacionais das pessoas para fins comerciais ou políticos, muitas vezes sem o seu conhecimento, limitando o exercício consciente da sua liberdade de escolha."

Trata-se de uma tecnologia emergente, caracterizada pela polivalência, que alcançou maior visibilidade a partir de 2016, altura em que a presidência japonesa do G7, colocou a IA na agenda, destacando as suas implicações e a necessidade de se garantir a proteção dos dados e a informação pessoal. Por essa altura, a União Europeia desenhava a sua estratégia sobre a IA, a que se seguiu um pacote legislativo em torno da proteção de dados pessoais, que veio a constituir um regime reforçado de proteção ao tratamento de dados sensíveis, onde se incluem os dados relativos à saúde. Posteriormente foram criadas regras harmonizadas dos sistemas de IA, da responsabilidade civil da IA, e governação europeia dos dados, numa tentativa de manter a vanguarda do percurso tecnológico mundial, ancorado num quadro ético e jurídico robusto, centrado no ser humano e na garantia dos direitos fundamentais.

O Santo Padre Francisco recorda-nos ainda que "a inteligência artificial deve ser entendida como uma galáxia de realidades diversas e não podemos presumir a priori que o seu desenvolvimento traga um contributo benéfico

para o futuro da humanidade e para a paz entre os povos. O resultado positivo só será possível se nos demonstrarmos capazes de agir de maneira responsável e respeitar valores humanos fundamentais como «a inclusão, a transparência, a segurança, a equidade, a privacidade e a fiabilidade»[557].

Por fim, torna-se obrigatória uma reflexão mais adensada sobre a vulnerabilidade humana face à aplicação de tecnologias computacionais inteligentes na saúde e à criação de prestadores de serviços de intermediação de dados, através da entrada em vigor do Regulamento da Governação Europeia de Dados, a 24 de setembro de 2023.

1. Sistemas de inteligência artificial baseados nos valores da União

Em 21 de abril de 2021, a Comissão Europeia publicou uma proposta de regulamento do Parlamento Europeu e do Conselho que veio estabelecer as regras harmonizadas em matéria de inteligência artificial[558]. Trata-se de um enquadramento jurídico dos sistemas de IA, baseado nos valores da União, consagrados na Carta dos Direitos Fundamentais da União Europeia (CDFUE), bem como na Convenção Europeia dos Direitos do Homem (CEDH).

Sob a Presidência espanhola do Conselho da União, no início de dezembro de 2023, o Conselho e o Parlamento chegaram a um acordo, ainda que provisório, sobre a proposta de regras harmonizadas em matéria de inteligência artificial (IA), apresentadas pela Comissão. O projeto de regulamento, que sofreu alterações face à proposta inicial, pretende garantir que os sistemas de IA colocados no mercado europeu e utilizados na União Europeia, não só ofereçam segurança e respeitem os direitos fundamentais e os valores da União, como também, estimulem o investimento e a inovação na Europa.

[557] FRANCISCO. Mensagem do Santo Padre para a celebração do Dia Mundial da Paz, 1 de janeiro de 2024.

[558] JOUE. Regulamento Inteligência Artificial. COM (2021) 206 final.

Os trabalhos técnicos continuaram tendo o regulamento sido aprovado a 2 de fevereiro de 2024. Até então, foi submetido ao *Coreper* (comité dos representantes dos Estados-Membros) para aprovação e, posteriormente confirmado e submetido à revisão jurídico-linguísticos, antes da sua publicação em 2024. O acordo previu uma *vacatio legis* de dois anos entre a publicação do diploma no Jornal Oficial da União Europeia e a sua entrada em vigor.

Fora do *Regulamento Inteligência Artificial* ficou a legislação relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial (Diretiva Responsabilidade Civil da IA)[559]. Também nesta matéria foi alcançado, no dia 14 de dezembro de 2023, um acordo político entre os Estados-Membros. Juntamente com o Regulamento Inteligência Artificial, a Diretiva Responsabilidade Civil da IA faz parte de um pacote de medidas destinadas a apoiar a implantação da IA na Europa mediante a promoção da excelência e da confiança. E, em virtude da inadequação das atuais regras nacionais de responsabilidade, em especial em matéria de responsabilidade culposa, ao tratamento de ações de indemnização por danos causados por produtos e serviços assentes em IA, a presente proposta oferece, às vítimas de danos causados pela IA, uma proteção equivalente à das vítimas de danos causados por produtos em geral, evitando a fragmentação das regras nacionais de responsabilidade civil específicas para a IA.

A inteligência artificial é uma família de técnicas de programação informática extremamente poderosas, que não obstante as inúmeras vantagens da sua aplicação, as características específicas de determinados sistemas de IA (incluindo a complexidade, a autonomia e a opacidade, o denominado efeito de «caixa negra») podem criar novos riscos relacionados com a segurança e a proteção, pôr em causa a vida privada e familiar, bem como a proteção dos dados pessoais, direitos fundamentais consagrados na Carta dos Direitos Fundamentais da União Europeia (CDFUE), bem como acelerar a probabilidade ou intensidade dos riscos existentes.

[559] JOUE. Diretiva Responsabilidade da IA. COM (2022) 496 final.

As Nações Unidas publicaram, em dezembro de 2023, o Relatório provisório: *Governing AI for Humanity*[560], que lança uma proposta para a governação internacional da IA, baseada na Carta das Nações Unidas e no seu compromisso para a paz, a segurança, os direitos humanos e o desenvolvimento sustentável, bem como na legislação internacional sobre Direitos Humanos. Nessa conformidade, deverá avaliar-se regularmente o estado da IA e a sua trajetória, harmonizar padrões, segurança e gestão de riscos, promover a colaboração multissetorial internacional, monitorar riscos e coordenar a resposta a emergências, bem como desenvolver normas vinculativas de responsabilização.

Neste contexto, recordemos Wolfgang Hoffmann-Riem, que na sua obra *Teoria Geral do Direito Digital, Transformação Digital Desafios para o Direito*, oferece-nos uma visão científica dos principais temas relacionados com o fenómeno da digitalização, bem como noções sólidas de «algoritmos», «inteligência artificial» e «*big data*». Com grande atualidade e pertinência, o autor aborda as regras técnicas, legais e sociais, contidas nos algoritmos digitais. Refere que os algoritmos são indispensáveis em quase todas as áreas da sociedade sendo, no entanto, uma descoberta problemática, pelos riscos que representa designadamente na manipulação de comportamentos e nas ameaças à privacidade[561].

Graças à convergência de fatores como o aumento da capacidade computacional, a multiplicação dos conjuntos de dados e a evolução dos algoritmos[562], a IA entrou numa nova era, transformando-se numa das áreas de investigação científica multidisciplinar mais complexas, atual e promissora. Esses progressos da ciência e da tecnologia oferecem grandes benefícios à humanidade, nomeadamente aumentando a esperança de vida e melhorando a sua qualidade. Porém, estes avanços devem ser guiados pela dignidade da pessoa humana e pelo respeito universal e efetivo dos direitos humanos e das liberdades fundamentais.

---

[560] NAÇÕES UNIDAS. *Interim Report: Governing AI* for Humanity, AI Advisory Body, dezembro 2023.

[561] HOFFMANN-REIM, WOLFGANG. *Teoria Geral do Direito Digital, Transformação Digital Desafios para o Direito,* p. 11-13.

[562] PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 20 de outubro de 2020, sobre os direitos de propriedade intelectual para o desenvolvimento de tecnologias ligadas à inteligência artificial.

Conscientes da transformação digital da sociedade, assumimos a relevância de incluir neste estudo, o setor da saúde, por se encontrar numa fase de grande carência, em toda a Europa. É comumente aceite que, face a uma população envelhecida e carenciada de serviços de saúde, não haverá profissionais de saúde suficientes para prestar os serviços que a população necessita. Além de mais, as aplicação das novas tecnologias (IA e robótica) no setor da saúde é altamente promissor, e contamos também com a confluência entre a revolução digital e a revolução genómica que abriu as portas à inovação neste setor. Em presença de todos estes avanços podemos concluir que vivemos um momento de esperança?

Reconhecendo que a saúde não depende apenas dos progressos da investigação científica e tecnológica, mas também de fatores psicossociais e culturais, e que as decisões relativas às questões éticas suscitadas pela medicina, pelas ciências da vida e pelas tecnologias que lhes estão associadas, podem ter repercussões sobre a humanidade em geral, procura-se contextualizar a forte transformação digital da saúde, de que resulta uma forte procura de soluções tendo por base a bioética, bem como a problematização das soluções de equidade.

Os riscos para a privacidade dos titulares dos dados de saúde, são elevados. Desse modo, ao aplicar todo o potencial tecnológico em áreas como "a telessaúde, a cirurgia robótica, o seguimento dos doentes via wearables ou a implementação de modelos preditivos para a decisão clínica, a segurança e a privacidade dos dados são primordiais"[563].

Em face das inquietações reveladas, fomos assistindo a debates, seminários sobre os desafios éticos da transformação digital, a proibição do tratamento de categorias especiais de dados pessoais, tal como prevê o n.º 1 do Art.º 9.º do Regulamento (UE) 2016/679, de 27 de abril (*RGPD*), Regulamento Geral de Proteção de Dados (*RGPD*)[564], bem como uma reflexão sobre a vulnerabilidade, conceito por muito tempo arredado do Direito, mas que defendemos neste estudo, trata-se de um conceito

[563] VITORINO., G; CORDEIRO, J.; MAGALHÃES, T., «A transformação digital nas suas diversas dimensões», in *Transformação digital em Saúde.* (2021).

[564] JOUE. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

ético-jurídico, tributário da bioética. Neste plano, importa recordar as palavras do Santo Padre Francisco, que recentemente nos alertava para a necessidade de serem criados modelos normativos, que ofereçam uma orientação ética aos criadores de tecnologias digitais. Nas suas palavras, o Santo Padre refere que,

> "é indispensável identificar os valores humanos que deveriam estar na base dos esforços das sociedades para formular, adotar e aplicar os quadros legislativos necessários. O trabalho de elaboração de diretrizes éticas para a produção de formas de inteligência artificial não pode prescindir da consideração de questões mais profundas relativas ao significado da existência humana, à proteção dos direitos humanos fundamentais, à busca da justiça e da paz. Este processo de discernimento ético e jurídico pode revelar-se preciosa ocasião para uma reflexão compartilhada sobre o papel que a tecnologia deveria ter na nossa vida individual e comunitária e sobre a forma como a sua utilização possa contribuir para a criação dum mundo mais equitativo e humano. Por este motivo, nos debates sobre a regulamentação da inteligência artificial, dever-se-ia ter em conta as vozes de todas as partes interessadas, incluindo os pobres, os marginalizados e outros que muitas vezes permanecem ignorados nos processos de decisão globais"[565].

Na perspetiva defendida no presente estudo, a aplicação das novas tecnologias nos vários domínios da nossa vida, deve assentar no princípio da dignidade da pessoa humana, princípio estruturante que se constitui como um farol, um fundamento ético-jurídico, um valor subjacente aos direitos fundamentais e reciprocamente influenciado pela autonomia pessoal, um princípio bioético que se traduz pela defesa da autodeterminação de cada pessoa em tomar decisões em relação à sua vida e em concreto à saúde.

Concretizando, o contributo da bioética para a autodeterminação da pessoa portadora de doença encontra-se presente, quer nos códigos deontológicos dos profissionais de saúde, quer nos instrumentos internacionais,

[565] FRANCISCO. Mensagem do Santo Padre para a celebração do Dia Mundial da Paz, 1 de janeiro de 2024.

como é exemplo a *Convenção sobre os Direitos do Homem e a Biomedicina,* ao plasmar no Art.º 5.º, que: «Qualquer intervenção no domínio da saúde só pode ser efectuada após ter sido prestado pela pessoa em causa o seu consentimento livre e esclarecido. Esta pessoa deve receber previamente a informação adequada quanto ao objectivo e à natureza da intervenção, bem como às suas consequências e riscos. A pessoa em questão pode, em qualquer momento, revogar livremente o seu consentimento».

2. Transformação dos municípios através da aplicação da IA na área da saúde

Tendo presente a tendência atual de uma população cada vez mais envelhecida, já anteriormente brevemente aflorada, assume-se como relevante, a Estratégia Nacional de Territórios Inteligentes (ENTI), aprovada pela Resolução do Conselho de Ministros n.º 176/2023, de 18 de dezembro, juntamente com o Plano de Ação da ENTI (2023-2030) e a Arquitetura de Referência para Plataformas de Gestão Urbana (ARPGU)[(566)].

Os instrumentos acima referidos mobilizam a atuação dos municípios em torno da oferta de cuidados de saúde. Porém, a "evolução de um ecossistema de territórios inteligentes para um ecossistema nacional inteligente", irá requer:

> "um processo de transformação nacional que inclui as áreas urbanas e não-urbanas, exigindo uma forte cooperação entre todos os atores relevantes, um alinhamento entre os interesses e prioridades nacionais, do setor público, empresas e sociedade e, uma integração e interoperabilidade entre os territórios de forma a criar valor e melhorar a qualidade de vida das pessoas. A contribuir para essa evolução estarão as tecnologias emergentes, tais como o 5G, *internet of things (IoT), cloud, edge computing,* realidade aumentada e virtual, inteligência artificial (IA), gémeos digitais, multiverso e analítica avançada, que irão amplificar o impulso estratégico de transformação dos territórios." (ENTI, p. 10,11)

[(566)] Agência para a Modernização Administrativa (AMA). Estratégia Nacional de Territórios Inteligente –ENTI (2023-2030), 2023.

A evolução de um ecossistema de territórios inteligentes assenta na utilização da IA aplicada a um conjunto de serviços públicos locais. A aplicação algorítmica irá exigir a agregação de dados em plataformas integradas, bem como a interoperabilidade desses mesmo dados. Nessa medida, quando em causa estejam dados pessoais e em especial dados pessoais sensíveis (dados de saúde e outros dados pessoais relativos às condições socioeconómicas das populações), serão consideradas operações de um risco elevado no âmbito do Regulamento Inteligência Artificial. Em face dos riscos associados à evolução pretendida, assume-se como necessário um grande investimento ao nível da arquitetura da infraestrutura tecnológica, de modo a cumprir as obrigações que resultam do referido regulamento. Segundo a ENTI,

> "O 5G pode e deve acelerar a coesão territorial através de uma Administração Pública mais próxima, que disponibiliza serviços públicos com soluções e canais adaptados às circunstâncias locais. Através da conjugação da possibilidade de medição em IoT, da capacidade de análise e tratamento avançado de dados, e da integração de modelos IA para extração de conhecimento, alavancadas na transmissão massiva de informação e em tempo real (5G). (...) Esta dimensão tecnológica inclui a agregação de dados e dos processos associados (recolha, tratamento, armazenamento, utilização e partilha) em plataformas integradas, garantindo a interoperabilidade dos vários sistemas relevantes neste contexto, através de interfaces de programação de aplicação (APIs)12 e serviços de integração". (ENTI, p. 11).

Relevante é o conjunto de Recomendações que a ENTI prevê e, que devem integrar os planos locais, podendo a sua aplicação ser ajustada pelo município e/ou Comunidades Intermunicipais/Áreas Metropolitanas (CIMs/AMs), consoante a maturidade que apresente. Entre os domínios mais relevantes em matéria de tratamento de dados relativos à saúde, sinalizamos os seguintes:

(i) "Sociedade inteligente, cuja recomendação consiste em: "Promover atividades de promoção da saúde e de inclusão social, de forma a

(567) *Application Programming Interfaces (APIs)*

promover a adoção de estilos de vida saudáveis e a prevenção de comportamentos de risco, assim como a requalificação de pessoas socialmente excluídas e ações no âmbito da rede de apoio social.

(ii) Qualidade de vida inteligente, que recomenda a adoção de: "Implementar parcerias entre municípios e entidades de saúde, em alinhamento com o Plano Nacional de Saúde 2030 e os Planos Locais de Saúde, contribuindo para a melhoria da saúde das populações e o reforço da acessibilidade, eficiência e diferenciação da oferta de cuidados de saúde de proximidade (telessaúde, teleassistência)" (ENTI, p. 18, 19).

Além da área da saúde, a ENTI consagra outras iniciativas com recurso à IA, igualmente promissoras.

Cumpre-nos recordar que a aplicação do Regulamento Inteligência Artificial visa garantir que os diferentes sistemas de IA colocados no mercado europeu, oferecem segurança e respeitam os direitos fundamentais. Relevante é o facto da IA passar a ser regulamentada com base na capacidade dos sistemas de IA causarem danos à sociedade. Compreende-se assim, que enquadramento legal da IA se baseie no risco, e estabeleça a diferença entre as utilizações que criam um risco inaceitável; um risco elevado e um risco baixo ou mínimo.

O Título II da proposta de Regulamento IA, consagra as práticas que determinam um *risco inaceitável,* ou seja, a aplicação dos sistemas IA proibidos[568]. As proibições, que foram expandidas no acordo provisório alcançado em dezembro de 2023, entre o Parlamento e o Conselho, prendem-se com práticas que visam manipular as pessoas, por meio de técnicas subliminares, sem que estas se apercebam, ou exploram as vulnerabilidades de grupos específicos, como as crianças ou as pessoas com deficiência, levando à alteração dos seus comportamentos de uma forma que seja suscetível de causar a si, ou a outra pessoa, danos psicológicos ou físicos[569].

---

[568] *Idem*, artigo 5.º.

[569] JOUE. COM (2021)206 final, p. 14.

Para além do alargamento das práticas de IA proibidas, o acordo provisório reafirmou as regras aplicáveis aos modelos de IA de finalidade geral e de grande impacto, que possam representar um risco sistémico no futuro, bem como os *sistemas de inteligência artificial de risco elevado* (Título III), para a saúde, segurança e direitos fundamentais das pessoas, designadamente os sistemas utilizados na gestão do tráfego rodoviário, no recrutamento ou seleção de pessoas, entre outros. Nestes casos estão previstos requisitos apertados dirigidos a estes sistemas de IA, impondo-se a necessidade de implementação de um sistema de gestão do risco e a obrigatoriedade de realização de uma avaliação de impacto sobre os direitos fundamentais, antes dos sistemas de IA serem colocados no mercado.

Por último, os fornecedores de sistemas de IA classificados de baixo risco, poderão aderir voluntariamente ao cumprimento dos requisitos estabelecidos no Regulamento através da criação e implementação dos seus próprios códigos de conduta, podendo incluir compromissos voluntários de sustentabilidade ambiental, tal como se prevê no Título IX.

Foi ainda revisto o sistema de governação, que é um dos quatro objetivos constantes do Título VI, no sentido de introduzir poderes de execução de forma a melhorar a governação e a aplicação do Regulamento e demais legislação em vigor em matéria de direitos fundamentais, bem como os requisitos de segurança aplicáveis aos sistemas de IA.

Do exposto, sublinha-se, que o quadro jurídico da IA será aplicável aos programas informáticos que permitem a aprendizagem automática; às abordagens baseadas na programação (lógica) indutiva, bases de conhecimento, motores de inferência e de dedução, sistemas de raciocínio (simbólico) e sistemas periciais, bem como abordagens estatísticas[570].

---

[570] *Vide* (Anexo I, Técnicas e Abordagens no domínio da IA, referidas no artigo 3.º, ponto 1) a) Abordagens de aprendizagem automática, incluindo aprendizagem supervisionada, não supervisionada e por reforço, utilizando uma grande variedade de métodos, designadamente aprendizagem profunda; b) Abordagens baseadas na lógica e no conhecimento, nomeadamente representação do conhecimento, programação (lógica) indutiva, bases de conhecimento, motores de inferência e de dedução, sistemas de raciocínio (simbólico) e sistemas periciais; c) Abordagens estatísticas, estimação de Bayes, métodos de pesquisa e otimização. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC_2&format=PDF

Importa ainda ter presente, que estão previstas regras e novas obrigações, no âmbito de uma aplicação alargada, que inclui a maioria dos intervenientes na cadeia de produção de IA, como fornecedores de IA, entidades que utilizam sistemas de IA, importadores, distribuidores, fabricantes de produto e representantes autorizados.

Apelidada de "emblemática", a iniciativa legislativa a publicar em 2024, tem o potencial de promover o desenvolvimento e a adoção de uma IA segura e fiável na União, por entidades públicas e privadas. Atendendo ao seu âmbito, o Regulamento Inteligência Artificial será aplicável às entidades, mesmo que não se encontrem estabelecidas na União Europeia, sendo apenas necessário que o sistema de IA seja colocado no mercado ou ao serviço do mercado europeu, ou ainda que o resultado produzido pelo sistema de IA seja utilizado na União Europeia[571].

3. Regras específicas relativas aos sistemas de IA aplicados à área da saúde

Vimos anteriormente que o Regulamento Inteligência Artificial consagra, no Título III, as regras específicas relativas aos sistemas de IA que criam um risco elevado para a saúde e a segurança ou para os direitos fundamentais de pessoas singulares.

A classificação de um sistema de IA como de risco elevado tem por base a finalidade para a qual foi criado o programa informático, em conformidade com a atual legislação relativa à segurança de produtos. Estes sistemas continuarão a ser autorizados no mercado europeu, mas sujeitam-se ao cumprimento de determinados requisitos obrigatórios e a uma avaliação da conformidade ex ante, em clara complementaridade com o *RGPD*.

Tomando por exemplo o *Digital Tracking and Tracing System* (DTTS), um sistema aparentemente criado para rastrear a propagação da COVID-19, foi altamente escortinado pelas Autoridades Nacionais de Proteção de Dados na Europa, tendo sido exigida uma apurada avaliação de impacto de proteção de dados *ex ante*, em conformidade com o Art.º 35.º do *RGPD*.

[571] JOUE. COM (2021)206 final, alínea c) do n.º 1 do artigo 2.º.

Retomando a complementaridade dos sistema de IA com o *RGPD,* dispõe o n.º 1 do Art.º 9.º, de um proibição geral do tratamento de dados relativos à saúde, protegendo estes dados com intensidade, por se tratar de categorias especiais de dados pessoais. Nessa categoria incluem-se as informações sobre a pessoa singular, recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, bem como qualquer número, símbolo ou sinal particular que lhe seja atribuído, a fim de a identificar de forma inequívoca para fins de cuidados de saúde. Integram-se ainda nesta categoria, as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a informação recolhida a partir de dados genéticos e amostras biológicas.

Integram-se ainda na categoria especial de dados pessoais relativos à saúde, qualquer informação relativa a uma doença, deficiência, risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, (médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico *in vitro*). Em todos os exemplos acima citados estamos a tratar dados pessoais sensíveis.

Um sistema de IA com a finalidade específica de tratamento dos dados sensíveis poderá materializar um risco elevado para uma pessoa concretamente identificada ou identificável, caso sejam incumpridos os requisitos legais relativamente aos dados e à governação de dados, à documentação e à manutenção de registos, à transparência e à prestação de informações aos utilizadores, à supervisão humana, à solidez, à exatidão e à segurança, tal como se encontram previstos no Capítulo 2 do Titulo III da Proposta do Regulamento Inteligência Artificial.

Não obstante os desafios identificados, a transformação digital dos serviços de saúde apresenta-se muito promissora. A esse propósito, recordemos o excelente trabalho do Grupo Independente de Peritos de Alto Nível sobre Inteligência Artificial (GPAN IA)[572], que em 2019, apresentou

[572] Grupo Independente de Peritos de Alto Nível sobre Inteligência Artificial, *Orientações éticas para uma inteligência artificial,* p. 14.

as *Orientações éticas para uma inteligência artificial.* Nesse documento, deu a conhecer vários projetos na área da saúde e do bem-estar, tais como: Projeto MURAB *(MRI and Ultrasound Robotic Assisted Biopsy)*; Projeto REVOLVER *(Repeated Evolution of Cancer)*; Projeto LIVE INCITE; Projeto CARESSES *(Culture-Aware Robots and Environmental Sensor Systems for Elderly Support)*; cujo tratamento inteligente foram determinantes para a prevenção de doenças potencialmente mortais.

Em suma, conscientes dos riscos para a confidencialidade, disponibilidade e integridade dos dados sensíveis associados à transformação digital na área da saúde, sublinhamos a relevância dos instrumentos jurídicos europeus referidos, em defesa dos direitos fundamentais e dos valores da União. Porém, dogmaticamente o tema da proteção de dados pessoais relativos à saúde obriga-nos a uma reflexão em contexto de regulação de múltiplos níveis, de construção e execução de instrumentos jurídicos europeus e internacionais. A esse propósito, voltamos ao Relatório provisório das Nações Unidas: *Governing AI for Humanity*[573], e em concreto, ao lançamento de uma proposta para a governação internacional da IA baseada na Carta das Nações Unidas e na legislação internacional sobre Direitos Humanos, o que nos leva a questionar se será possível a criação de uma norma mundial para a aplicação da IA na área da saúde?

4. Privacidade e confidencialidade dos dados sensíveis em contexto multinível

A privacidade e a confidencialidade dos dados sensíveis, onde se incluem os dados de saúde, e em concreto os dados genéticos, encontram consagração, no n.º 1 do Art.º 9.º do *RGPD*, e em outros instrumentos jurídicos internacionais, designadamente na *Declaração Internacional sobre os Dados Genéticos Humanos,* adotada pela Conferência Geral da UNESCO em 16 de outubro de 2003[574], que no seu Art.º 14.º alínea b) refere, que,

[573] NAÇÕES UNIDAS. *Interim Report: Governing AI for Humanity, AI Advisory Body*, dezembro 2023.

[574] Declaração Internacional sobre os Dados Genéticos Humanos, 16 de outubro de 2003.

"Os dados genéticos humanos[575], os dados proteómicos humanos[576] e as amostras biológicas[577] associados a uma pessoa identificável não deverão ser comunicados nem tornados acessíveis a terceiros, em particular empregadores, companhias de seguros, estabelecimentos de ensino ou família, se não for por um motivo de interesse público importante nos casos restritivamente previstos pelo direito interno em conformidade com o direito internacional relativo aos direitos humanos, ou ainda sob reserva de consentimento prévio, livre, informado e expresso da pessoa em causa, na condição de tal consentimento estar em conformidade com o direito interno e com o direito internacional relativo aos direitos humanos. A vida privada de um indivíduo que participa num estudo em que são utilizados dados genéticos humanos, dados proteómicos humanos ou amostras biológicas deverá ser protegida e os dados tratados como confidenciais".

Relativamente à informação genética, o Conselho Nacional de Ética para as Ciências da Vida (CNECV) emitiu um parecer[578] aquando da ratificação do Protocolo Adicional à CDHBM[579] no qual exprime "alguma preocupação relativamente ao uso impróprio dos testes genéticos, quando não são usados para fins relacionados com a saúde e quando não são enquadrados por consultas de aconselhamento genético, pelo que se pretende assegurar a proteção

---

[575] Dados genéticos humanos: informações relativas às características hereditárias dos indivíduos, obtidas pela análise de ácidos nucleicos ou por outras análises científicas; [Declaração Internacional sobre os Dados Genéticos Humanos, artigo 2.º (i)].

[576] Dados proteómicos humanos: informações relativas às proteínas de um indivíduo, incluindo a sua expressão, modificação e interação; [Declaração Internacional sobre os Dados Genéticos Humanos, artigo 2.º (ii)].

[577] Amostra biológica: qualquer amostra de material biológico (por exemplo células do sangue, da pele e dos ossos ou plasma sanguíneo) em que estejam presentes ácidos nucleicos e que contenha a constituição genética característica de um indivíduo; [Declaração Internacional sobre os Dados Genéticos Humanos, artigo 2.º (iv)].

[578] Conselho Nacional de Ética para as Ciências da Vida (CNECV). Relatório e Parecer sobre a ratificação do Protocolo Adicional à Convenção para a Proteção dos Direitos do Homem e a Biomedicina (CDHBM) referente aos Testes Genéticos para fins relacionados com a Saúde, 84/CNECV/2015.

[579] Portugal assinou em 17 de março de 2015.

da informação obtida através da sua realização" (p. 7). Não obstante essa apreciação, o CNECV deu parecer favorável aos valores éticos acolhidos no Protocolo Adicional à CDHBM, que sublinha o respeito pelos princípios do primado do ser humano, da não discriminação, da não estigmatização e da reserva da vida privada (p. 8). Não obstante os receios manifestados, o referido Protocolo enfatiza os benefícios decorrentes da genética, nomeadamente dos testes genéticos, abrindo caminho para o que se designa por "medicina de precisão" ou "medicina personalizada".

Tal como aludido anteriormente, no plano europeu, o sector da saúde assume uma especial relevância em matéria de proteção de dados pessoais, e no Art.º 9º n.º 1 do *RGPD* foi consagrado o princípio geral da proibição de tratamento de determinadas categorias especiais de dados, como os genéticos, biométricos, relativos à saúde ou relativos à vida sexual ou orientação sexual de uma pessoa.

A informação de saúde integra, nos termos do *RGPD* uma categoria especial de dados pessoais que são objeto de especial proteção. Porém, à luz das exceções previstas no n.º 2 do Art.º 9.º, tanto os dados de saúde, como os dados genéticos podem ser tratados quando se aplique um dos seguintes fundamentos de licitude:

- Consentimento explícito do utente/portador de doença; [alínea a) do n.º 2 do Art.º 9.º do *RGPD*];
- Proteção de interesses vitais do utente ou de um terceiro, no caso de o titular dos dados estar fisicamente ou legalmente incapacitado de dar o seu consentimento [alínea c) do n.º 2 do Art.º 9.º do *RGPD*];
- Medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamento de saúde e para gestão de sistemas e serviços de saúde; [alínea h) do n.º 2 do Art.º 9.º do *RGPD*];
- Interesse público no domínio da saúde pública [alínea i) do n.º 2 do Art.º 9.º *RGPD*].

Importa, no entanto, considerar que a cedência e/ou portabilidade da informação de saúde não pode, à luz do ordenamento jurídico vigente, ser considerado um ato meramente administrativo, que possa ser confiado ou executado por um funcionário do secretariado Importa, no entanto, considerar que a cedência e/ou portabilidade da informação de saúde não pode, à luz do ordenamento jurídico vigente, ser considerado um ato meramente administrativo, que possa ser confiado ou executado por um funcionário do secretariado administrativo, pois o mesmo envolve, em primeiro lugar, decisões quanto ao preenchimento dos requisitos jurídicos de legitimidade, depois decisões médicas quanto à aplicação ou não do conceito de privilégio terapêutico e, finalmente, uma seriação daquelas que são as anotações pessoais dos médicos e as informações prestadas por terceiros e/ou relativas a terceiros.

O *RGPD* introduziu alterações significativas com implicações estruturais no funcionamento das organizações, que não cabe no âmbito do presente estudo, exigindo aos prestadores de cuidados de saúde, independentemente da sua natureza jurídica ou dimensão, uma adequação exigente e cuidada dos seus processos de tratamento de dados pessoais, sempre visando a garantia dos direitos e liberdades dos titulares desses dados.

5. Princípios éticos aplicáveis à prática clínica à investigação médica

A *Declaração de Helsínquia, Princípios Éticos para a Investigação Médica em Seres Humanos* (versão de outubro 2013), defende que devem ser tomadas todas as precauções para proteger a privacidade de cada sujeito de investigação e a confidencialidade dos seus dados pessoais. No mesmo sentido, a *Convenção para a Proteção dos Direitos do Homem e da Dignidade do Ser Humano face às aplicações da Biologia e da Medicina: Convenção sobre os Direitos do Homem e a Biomedicina (CDHBM)*[580], dispõe no Art.º 1.º que «As Partes na presente Convenção protegem o ser humano na sua

[580] Convenção para a Proteção dos Direitos do Homem e da Dignidade do Ser Humano face às aplicações da biologia e da medicina: convenção sobre os direitos do homem e a biomedicina.

dignidade e na sua identidade e garantem a toda a pessoa, sem discriminação, o respeito pela sua integridade e pelos seus outros direitos e liberdades fundamentais face às aplicações da biologia e da medicina.» e no Art.º 3.º prevê o acesso equitativo no acesso à saúde de qualidade apropriada.

Dos estudos realizados, verifica-se que os dilemas éticos na prática clínica provocados pelos avanços da ciência constituem a regra, quando outrora eram a exceção. No presente, são "enfrentados por todos os profissionais que se dedicam à prática da arte médica".[581] Esses dilemas têm exigido uma maior atuação de "comités de ética" ou "conselhos de éticas" nas instituições, bem como a criação de códigos de ética, que orientam o cumprimento dos padrões éticos e legais, pelos profissionais de saúde, bem como o cumprimento da legislação aplicável à investigação científica.

A *Declaração de Helsínquia da Associação Médica Mundial sobre os Princípios Éticos Aplicáveis às Investigações Médicas sobre Sujeitos Humanos,* adotada em 1964[582], na versão atual, ocupa-se desta temática e reforça que «A investigação médica está sujeita a padrões éticos que promovem e garantem o respeito por todos os seres humanos e protegem a sua saúde e direitos». (nº 7). A Declaração enuncia que, «Embora o objetivo primário da investigação médica seja gerar novo conhecimento, essa finalidade nunca prevalece sobre os direitos e interesses individuais dos participantes na investigação» (n.º 8). Sustenta ainda que, é um «dever dos médicos que participam em investigação médica proteger a vida, a saúde, a dignidade, a integridade, o direito à autodeterminação, a privacidade e a confidencialidade da informação pessoal dos participantes.» (n.º 9). É ao médico e ao profissional de saúde que cabe a responsabilidade de proteger os participantes sujeitos de investigação, não sendo aceitável a transferência para o sujeito de investigação, mesmo que este tenha dado consentimento.

---

[581] MARQUES FILHO, J. Bioética Clínica – Cuidando de Pessoas, Clinical Bioethics, p. 32.

[582] ASSOCIAÇÃO MÉDICA MUNDIAL. Declaração de Helsínquia sobre os princípios éticos aplicáveis às investigações médicas sobre sujeitos humanos, adotada em 1964.

O progresso da ciência assenta na investigação clínica, sendo defensável que os benefícios daí resultantes, devam ser partilhados com a sociedade no seu todo e, em particular com os países em desenvolvimento. Partindo dessa premissa, a *Declaração Universal sobre Bioética e Direitos Humanos,* adotada pela Conferência Geral da UNESCO em 11 de novembro de 1997, apresenta as várias formas de concretizar esses benefícios, designadamente através do acesso a cuidados de saúde de qualidade; fornecimento de novos produtos e meios terapêuticos ou diagnósticos, resultantes da investigação e apoio aos serviços de saúde.

A saúde é essencial à própria vida e deve ser considerada um bem social e humano. A *Declaração Universal sobre o Genoma Humano e os Direitos Humanos*[583], alude aos benefícios dos progressos nas áreas da biologia, da genética e da medicina, relativos ao genoma humano, defendendo que esses benefícios «serão postos à disposição de todos, tendo devidamente em conta a dignidade e os direitos humanos de cada pessoa». (al a) Art.º 12.º).

O Santo Padre Francisco recorda-nos "que a pesquisa científica e as inovações tecnológicas não estão desencarnadas da realidade nem são «neutrais»[584], mas estão sujeitas às influências culturais. Sendo atividades plenamente humanas, os rumos que tomam refletem opções condicionadas pelos valores pessoais, sociais e culturais de cada época. E o mesmo se diga dos resultados que alcançam: enquanto fruto de abordagens especificamente humanas do mundo envolvente, têm sempre uma dimensão ética, intimamente ligada às decisões de quem projeta a experimentação e orienta a produção para objetivos particulares"[585].

A *Declaração de Helsínquia da Associação Médica Mundial sobre os Princípios Éticos Aplicáveis às Investigações Médicas sobre Sujeitos Humanos,* adotada em 1964, anteriormente referida, defende que o «O objetivo

---

[583] Declaração Universal sobre o Genoma Humano e os Direitos Humanos.

[584] FRANCISCO, Carta enc. Laudato si' (24/V/2015), 114, in Mensagem do Dia Mundial da Paz, 01 de janeiro de 2024.

[585] FRANCISCO. Mensagem do Santo Padre para a celebração do Dia Mundial da Paz, 1 de janeiro de 2024.

primário da investigação médica em seres humanos é compreender as causas, a evolução e os efeitos das doenças e melhorar as intervenções preventivas, diagnósticas e terapêuticas (métodos, procedimentos e tratamentos). Mesmo as melhores e mais comprovadas intervenções atuais têm de ser continuadamente avaliadas através de investigação sobre a sua segurança, eficácia, eficiência, acessibilidade e qualidade» (n.º 6). No mesmo sentido, a *Declaração Universal sobre o Genoma Humano e os Direitos Humanos*[586], defende que «Nenhuma investigação na área do genoma humano ou respetivas aplicações, em particular nas áreas da biologia, da genética e da medicina, deve prevalecer sobre o respeito pelos direitos humanos, pelas liberdades fundamentais e pela dignidade das pessoas ou, se for caso disso, dos grupos de pessoas.» (Art.º 10.º)[587].

A Associação Médica Mundial (AMM) elaborou a Declaração de Helsínquia como um enunciado de princípios éticos para a investigação clínica envolvendo seres humanos, incluindo investigação sobre dados e material humano identificáveis. De entre esses princípios, destaca-se o *princípio da integridade da investigação,* motivado pela consciência da existência de casos de violação da transparência, qualidade e integridade da investigação científica. Pelos mesmos motivos, na última revisão da Declaração de Helsínquia, Princípios Éticos para a Investigação Médica em Seres Humanos (2013), os aspetos da investigação científica feita em seres humanos, mormente nos n.os 35 e 36, foram enfatizados[588].

O Regulamento europeu sobre ensaios clínicos de medicamentos de uso humano (Regulamento (UE) N.º 536/2014 do Parlamento Europeu e do Conselho de 16 de abril de 2014), exige a garantia, robustez e fiabilidade do ensaio. Com efeito, a ética da investigação visa os seguintes objetivos: (i) defender a correção dos dados recolhidos; (ii) assegurar o prestígio e a qualidade da investigação clínica; (iii) garantir a qualidade

---

[586] Declaração Universal sobre o Genoma Humano e os Direitos Humanos.

[587] *Idem Ibidem.*

[588] ASSOCIAÇÃO MÉDICA MUNDIAL. Declaração de Helsínquia sobre os princípios éticos aplicáveis às investigações médicas sobre sujeitos humanos, adotada em 1964.

dos produtos ou processos (maxime medicamentos) que resultam do estudo clínico e ainda a segurança e a saúde dos próprios participantes no ensaio clínico.

O princípio da integridade da investigação possui duas dimensões: (i) ao nível "supra-individual", fazendo o contraponto com o princípio do respeito pela intimidade da vida privada e familiar; (ii) ao nível pessoal--individual que participa no estudo clínico, obrigando a uma ponderação ética entre dois interesses ou valores da própria pessoa que consentiu participar num estudo clínico. Daqui resulta a possibilidade de interesses conflituantes (individual/comunitários), sendo admitido pela ética em investigação, o imperativo segundo o qual o bem-estar da sociedade e da ciência não prevalecem sobre o bem-estar do indivíduo, em conformidade com o Art.º 2.º da Convenção sobre os Direitos do Homem e a Biomedicina, que aí consagra o «primado do ser humano». No mesmo sentido, «Embora o objetivo primário da investigação médica seja gerar novo conhecimento, essa finalidade nunca prevalece sobre os direitos e interesses individuais dos participantes na investigação». (n.º 8 da Declaração de Helsínquia).

6. Bioética e o princípio da autonomia: o consentimento informado

O contributo da bioética para a autodeterminação da pessoa foi por nós abordado numa fase inicial do presente estudo. Aí ficou vertido, que a aplicação das novas tecnologias nos vários domínios da nossa vida, deve assentar no princípio da dignidade da pessoa humana, princípio estruturante que é reciprocamente influenciado pela autonomia pessoal, um princípio bioético que se traduz na defesa da autodeterminação de cada pessoa, em tomar decisões em relação à sua vida e em concreto à saúde.

Porém, o exercício da razão moral e da autodeterminação é condicionada por fatores diversos, de índole biológica, económica e social, sendo necessário atender a todos os elementos de ordem social e às demais fragilidades do ser humano. Ou seja, à luz do princípio da autonomia do ser humano extraímos uma regra geral sobre o consentimento.

A esse propósito, o Regulamento n.º 707/2016, de 21 de julho, Regulamento de Deontologia Médica, refere no Art. 20.º que, «O consentimento do doente só é válido se este, no momento em que o dá, tiver capacidade de decidir livremente, se estiver na posse da informação relevante e se for dado na ausência de coações físicas ou morais.». Ou seja, o princípio da autonomia releva, mesmo nas situações de maior vulnerabilidade e dependência.

A *Convenção sobre os Direitos do Homem e a Biomedicina,* prevê no Art.º 5.º que, «Qualquer intervenção no domínio da saúde só pode ser efectuada após ter sido prestado pela pessoa em causa o seu consentimento livre e esclarecido. Esta pessoa deve receber previamente a informação adequada quanto ao objectivo e à natureza da intervenção, bem como às suas consequências e riscos. A pessoa em questão pode, em qualquer momento, revogar livremente o seu consentimento». No mesmo sentido, o Art.º 6.º da *Declaração Universal sobre Bioética e Direitos Humanos,* sublinha que,

> «1. Qualquer intervenção médica de carácter preventivo, diagnóstico ou terapêutico só deve ser realizada com o consentimento prévio, livre e esclarecido da pessoa em causa, com base em informação adequada. Quando apropriado, o consentimento deve ser expresso e a pessoa em causa pode retirá-lo a qualquer momento e por qualquer razão, sem que daí resulte para ela qualquer desvantagem ou prejuízo.
>
> 2. Só devem ser realizadas pesquisas científicas com o consentimento prévio, livre e esclarecido da pessoa em causa. A informação deve ser suficiente, fornecida em moldes compreensíveis e incluir as modalidades de retirada do consentimento. A pessoa em causa pode retirar o seu consentimento a qualquer momento e por qualquer razão, sem que daí resulte para ela qualquer desvantagem ou prejuízo. Excepções a este princípio só devem ser feitas de acordo com as normas éticas e jurídicas adoptadas pelos Estados e devem ser compatíveis com os princípios e disposições enunciados na presente Declaração, nomeadamente no Art.º 27º, e com o direito internacional relativo aos direitos humanos».

A *Declaração Internacional sobre os Dados Genéticos Humanos,* no seu Art.º 8.º refere que «(a) O consentimento prévio, livre, informado e expresso, sem tentativa de persuasão por ganho pecuniário ou outra vantagem pessoal, deverá ser obtido para fins de recolha de dados genéticos humanos, de dados proteómicos humanos ou de amostras biológicas, quer ela seja efectuada por métodos invasivos ou não-invasivos, bem como para fins do seu ulterior tratamento, utilização e conservação, independentemente de estes serem realizados por instituições públicas ou privadas. Só deverão ser estipuladas restrições ao princípio do consentimento por razões imperativas impostas pelo direito interno em conformidade com o direito internacional relativo aos direitos humanos».

No mesmo sentido, o *RGPD* prevê no Art.º 7.º as condições aplicáveis ao consentimento, sendo exigido ao responsável pelo tratamento não somente a prova da recolha do consentimento, mas igualmente a prova "que o consentimento foi efetivamente assentido"[589].

7. Vulnerabilidade como um conceito ético-jurídico

As questões éticas suscitadas pela medicina, ciências da vida e tecnologias associadas na sua aplicação aos seres humanos abordadas anteriormente, estão previstas na *Declaração Universal sobre Bioética e Direitos Humanos,* adotada em 2005[590], instrumento que foi concebido em defesa do pleno respeito pela dignidade humana, direitos humanos e liberdades fundamentais.

Ao consagrar a bioética entre os direitos humanos internacionais e ao garantir o respeito pela vida dos seres humanos, a Declaração defende que « Os interesses e o bem-estar do indivíduo devem prevalecer sobre o interesse exclusivo da ciência ou da sociedade.» (n.º 2 do Art.º 3.º).

Reconhece a interligação que existe entre ética e direitos humanos no domínio específico da bioética e defende a maximização dos efeitos benéficos diretos e indiretos dos avanços dos conhecimentos científicos,

[589] MENEZES CORDEIRO. 2021.p.121.

[590] Declaração Universal sobre Bioética e Direitos Humanos.

da prática médica e das tecnologias que lhes estão associadas, aplicando-os aos doentes, participantes em investigações e outros indivíduos envolvidos, devendo minimizar qualquer efeito nocivo suscetível de afetar esses indivíduos (Art.º 4.º).

A Declaração consagra o respeito pela vulnerabilidade humana e integridade pessoal no Art.º 8.º, prevendo aí que «Na aplicação e no avanço dos conhecimentos científicos, da prática médica e das tecnologias que lhes estão associadas, deve ser tomada em consideração a vulnerabilidade humana. Os indivíduos e grupos particularmente vulneráveis devem ser protegidos, e deve ser respeitada a integridade pessoal dos indivíduos em causa».

No plano nacional, a Constituição da República Portuguesa (CRP) acolhe no Art.º 1.º a dignidade da pessoa humana, princípio que acompanha o percurso vital de cada pessoa, nas suas múltiplas circunstâncias. Mariana Canotilho defende que "A *pessoa* constitucional é uma pessoa que *muda,* evolui e se transforma, passando por períodos de maior fragilidade, ou *vulnerabilidade,* mais ou menos duradouros, em que, à semelhança dos períodos da infância, juventude e terceira idade, necessita de uma *especial proteção constitucional, de direitos fundamentais específicos* e de políticas públicas próprias. São óbvios exemplos destas situações a deficiência (Art.º 71.º da CRP), a gravidez, maternidade e paternidade (Art.os 36.º e 68.º) e a doença (Art.º 64.º da CRP)"[591]. A autora refere as inúmeras disposições normativas positivadas no texto constitucional que se destinam a conferir direitos pessoais, laborais e de cidadania a qualquer pessoa. Na visão da autora, que acompanhamos de perto,

> "(...) A pessoa constitucional é, assim, multidimensional. Tem um nome, uma identidade, uma imagem (veja-se o Art.º 26.º da CRP); vive em família (Art.º 36.º), organiza-se em associações de diversa natureza (Art.º 46.º); instrui-se, aprende (Art.os 43.º, e 73.º a 76.º da CRP);

[591] CANOTILHO, Mariana. 2022, p. 146.

trabalha (e, neste ponto, acentue-se a relevância fulcral do trabalho, no texto e no projeto político da Constituição, que se reflete no número e densidade de disposições constitucionais sobre a matéria, desde logo, todo o Capítulo III do Título II – direitos, liberdades e garantias dos trabalhadores, e os Art.os 58.º e 59.º da CRP)"[592].

A vulnerabilidade humana é uma condição universal reconhecida também pela *Declaração Universal sobre o Genoma Humano os Direitos Humanos* (adotada pela Conferência Geral da UNESCO em 11 de novembro de 1997), que defende igualmente o direito à saúde como um dos direitos fundamentais de qualquer ser humano, " Reconhecendo que a investigação sobre o genoma humano e suas consequentes aplicações abre amplas perspetivas de progresso ao nível da melhoria da saúde dos indivíduos e da Humanidade no seu conjunto, mas sublinhando que tal investigação deve respeitar plenamente a dignidade humana, a liberdade e os direitos humanos, bem como a proibição de todas as formas de discriminação com base nas características genéticas,[593] .

Os fundamentos expostos permitem-nos observar que a pessoa humana é um sujeito livre e racional, mas também vulnerável e dependente, designadamente em caso de doença, cuja vulnerabilidade convoca a intervenção do Estado na prestação de cuidados de saúde, destacando-se em Portugal, o Serviço Nacional de Saúde e mais recentemente com uma forte mobilização por parte dos municípios.

8. Governação Europeia de Dados

Existe uma apreensão relativa à eventual vulnerabilidade dos titulares dos dados pessoais, e em especial dos dados relativos à saúde, face à criação dos prestadores de serviços de intermediação de dados, em execução do Regulamento (UE) 2022/868, de 30 de maio de 2022 (Governação Europeia de Dados)[594].

Se por um lado, com este novo instrumento que entrou em vigor no dia 24 de setembro de 2022, se procura reforçar a capacidade de ação dos titulares dos dados, nomeadamente o controlo que os titulares exercem

[593] Declaração Universal dos Direitos Humanos (DUDH).

[594] JOUE. Regulamento (UE) 2022/868 de 30 de maio de 2022.

sobre os dados que lhes dizem respeito, por outro lado, faltam definir os requisitos relativos à fiabilidade da prestação dos serviços de intermediação de dados, necessários à segurança do tratamento dos dados, de modo a assegurar que os titulares dos dados e detentores dos dados, bem como os utilizadores de dados, exerçam o controlo sobre o acesso e a utilização dos seus dados, em conformidade com o direito da União.

Em termos gerais, os serviços de intermediação de dados e, em concreto dos dados pessoais relativos à saúde, irão desempenhar um papel fundamental na sociedade, com potencial para a mutualização eficiente desses dados, bem como uma maior facilidade de partilha bilateral de dados. O *considerando* 27 do Regulamento de Governação Europeia de Dados dispõe que, "(...) Os serviços de intermediação de dados poderão incluir as partilhas bilaterais ou multilaterais de dados ou a criação de plataformas ou de bases de dados que permitam a partilha ou a utilização conjunta de dados, bem como a criação de uma infraestrutura específica para a interligação dos titulares dos dados e dos detentores dos dados com os utilizadores de dados." Trata-se de ativos que irão permitir a reutilização dos dados detidos por um organismo do setor público, realizada para fins comerciais, que não correspondem à finalidade inicial da missão de serviço público para a qual os dados foram produzidos e carece de mais informação relativamente à execução de interfaces técnicas e às condições técnicas e organizativas a aplicar.

A autoridade de controlo (a criar), poderá exigir a garantia que não existem incentivos desajustados que levem os titulares dos dados a utilizar esses serviços para disponibilizar informação, contra os seus próprios interesses. Tal poderá passar por informação a disponibilizar aos cidadãos, incluindo o aconselhamento sobre as utilizações possíveis dos seus dados, a fim de evitar práticas fraudulentas.

Um elemento fundamental para instaurar a confiança e aumentar o controlo, por parte dos detentores dos dados, dos titulares dos dados e dos utilizadores dos dados, relativamente aos serviços prestados, passa pela garantia de neutralidade dos prestadores de serviços de intermediação de dados no que diz respeito aos dados trocados entre os detentores dos dados ou os titulares dos dados e os utilizadores dos dados.

Por conseguinte, os prestadores de serviços de intermediação de dados, devem atuar como intermediários nas transações e não utilizar os dados trocados para qualquer outro fim.

O serviço de intermediação de dados pessoais relativos à saúde insere-se numa categoria específica de serviços de intermediação de dados. Estes prestadores de serviços procuram reforçar a capacidade de ação dos titulares dos dados, nomeadamente o controlo que as pessoas exercem sobre os dados que lhes dizem respeito. Nessa medida, para que se constitua como prestador de serviços de intermediação de dados relativos à saúde[595], sob jurisdição do Estado português, ser-lhe-á exigido: (i) a exequibilidade dos direitos dos titulares constantes do Capítulo III do Regulamento (UE) 2016/679, de 27 de abril (*RGPD*), nomeadamente o direito de dar e retirar o seu consentimento para o tratamento dos dados, o direito de acesso aos dados de que são titulares, o direito à retificação de dados pessoais inexatos, o direito ao apagamento dos dados ou o direito «a ser esquecido», o direito à limitação do tratamento e o direito à portabilidade dos dados, que permite aos titulares transferir os seus dados pessoais de um responsável pelo tratamento de dados para outro; (ii) a observância do procedimento de notificação à autoridade competente; (iii) a submissão ao controlo e supervisão do cumprimento dos requisitos previstos no Capítulo III do Regulamento de Governação Europeia de Dados.

A fim de aplicar o quadro de governação europeia de dados, foi criado o Comité Europeu da Inovação de Dados *(European Data Innovation Board),* sob a forma de um grupo de peritos, o qual irá facilitar a partilha de boas práticas em matéria de intermediação de dados, bem como, definir as prioridades em matéria de normas de interoperabilidade intersectoriais.

---

[595] Qualquer prestador de serviços de intermediação de dados, deve seguir os modelos constantes do anexo do Regulamento de execução (UE) 2023/1622 da Comissão de 9 de agosto de 2023, relativo à conceção de logótipos comuns para identificar os prestadores de serviços de intermediação de dados e as organizações de altruísmo de dados reconhecidos na União, que entrou em vigor em 2023, e está acessível em: «https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32023R1622». Importa nesta matéria referir que Portugal já tornou público o seu logótipo, acessível em: «https://digital-strategy.ec.europa.eu/en/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union». A Comissão Europeia manterá um registo central dos intermediários de dados reconhecidos.

De acordo com o *considerando* 53 do Regulamento de Governação Europeia de Dados, o Comité Europeu da Inovação de Dados[596] deverá ser composto por representantes das autoridades competentes para serviços de intermediação de dados, bem como por vários subgrupos, incluindo um subgrupo para a participação das partes interessadas, composto por representantes pertinentes da indústria, como a saúde, o ambiente, a agricultura, os transportes, a energia, a indústria transformadora, os meios de comunicação social, os setores cultural e criativo e as estatísticas, bem como por representantes da investigação, do meio académico, da sociedade civil, dos organismos de normalização, dos espaços comuns europeus de dados pertinentes e de outras partes interessadas e terceiros pertinentes, nomeadamente organismos com competências específicas, como os serviços nacionais de estatística.

Considerações finais

Sob a Presidência espanhola do Conselho da União, no início de dezembro de 2023, o Conselho e o Parlamento chegaram a um acordo, ainda que provisório, sobre regras harmonizadas em matéria de inteligência artificial (IA). Os trabalhos técnicos continuaram, tendo o regulamento sido aprovado no dia 2 de fevereiro de 2024.

O Regulamento visa garantir que os sistemas de IA colocados no mercado europeu e utilizados na União Europeia, ofereçam segurança e respeitem os direitos fundamentais, bem como os valores da União, estimule o investimento e a inovação na Europa. Fora do Regulamento Inteligência Artificial ficou a legislação relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial (Diretiva Responsabilidade Civil da IA). Também nesta matéria foi alcançado, no dia 14 de dezembro de 2023, um acordo político entre os Estados-Membros.

---

[596] O Comité Europeu da Inovação de Dados reuniu pela primeira vez no dia 13 de dezembro de 2023, informação que poderá ser acedida em: «https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3903».

O novo contexto, traz obrigatoriamente ao debate os desafios éticos da transformação digital, a proibição do tratamento de categorias especiais de dados pessoais, bem como uma reflexão sobre a vulnerabilidade como um conceito ético-jurídico. Dos estudos realizados, verifica-se que os dilemas éticos na prática clínica provocados pelos avanços da ciência constituem a regra, quando outrora eram a exceção. Esses dilemas têm exigido uma maior atuação de "comités de ética" ou "conselhos de éticas" nas instituições, bem como a criação de códigos de ética, que orientam o cumprimento dos padrões éticos e legais, pelos profissionais de saúde, bem como o cumprimento da legislação aplicável à investigação científica.

Cumpre-nos sublinhar que a pessoa humana é um sujeito livre e racional, mas também vulnerável e dependente, designadamente em caso de doença, cuja vulnerabilidade convoca em Portugal, a intervenção do Estado na prestação de cuidados de saúde, destacando-se em particular o Serviço Nacional de Saúde, tendo a Estratégia Nacional de Territórios Inteligentes (ENTI), mobilizado a atuação dos municípios em torno da oferta de cuidados de saúde.

Por fim, uma nota à apreensão relativa à eventual vulnerabilidade dos titulares dos dados pessoais, e em especial os dados relativos à saúde, face à criação dos prestadores de serviços de intermediação de dados, em execução do Regulamento Governação Europeia de Dados. Se por um lado, esse instrumento procura reforçar o controlo que os titulares exercem sobre os dados que lhes dizem respeito, por outro lado, não foram ainda definidos os requisitos relativos à fiabilidade da prestação dos serviços de intermediação de dados.

Referências

AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA (AMA). Estratégia Nacional de Territórios Inteligentes- ENTI (2023-2030), Área Governativa da Digitalização e da Modernização Administrativa. Dezembro 2023. Disponível em: HTTPS://WWW.AMA.GOV.PT/DOCUMENTS/24077/320185/ENTI_RCM_V2_ATUALIZADO.PDF/634A2167-0E64-48E5-9DDC-EF1FD3FC0CA8

ASSOCIAÇÃO MÉDICA MUNDIAL. Declaração de Helsínquia sobre os princípios éticos aplicáveis às investigações médicas sobre sujeitos humanos, adotada em 1964. Disponível em: https://www.ucp.pt/sites/default/files/2019-03/declaracao-de-helsinquia_2013.pdf

CANOTILHO, Mariana. «A vulnerabilidade como conceito constitucional: Um elemento para a construção de um constitucionalismo do comum», OÑATI SOCIO-LEGAL SERIES VOLUME 12, ISSUE 1 (2022), 138–163 publicado em fevereiro de 2022, p. 146. Disponível em: file:///C:/Users/cristina.caldeira/Downloads/pdf-12-1-canotilho-osls%20(3).pdf

CONSELHO NACIONAL DE ÉTICA PARA AS CIÊNCIAS DA VIDA (CNECV). Relatório e Parecer sobre a ratificação do Protocolo Adicional à Convenção para a Proteção dos Direitos do Homem e a Biomedicina (CDHBM) referente aos Testes Genéticos para fins relacionados com a Saúde, 84/CNECV/2015. Disponível em: https://www.cnecv.pt/pt/deliberacoes/pareceres/parecer-n-o-84-cnecv-2015-sobre-a-ratificacao-do-protocolo-adici?download_document=3202&token=e848d37cdb49de5145fcffa922383687

CONVENÇÃO PARA A PROTEÇÃO DOS DIREITOS DO HOMEM E DA DIGNIDADE DO SER HUMANO face às aplicações da biologia e da medicina: convenção sobre os direitos do homem e a biomedicina. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/convencao_protecao_dh_biomedicina.pdf

DECLARAÇÃO INTERNACIONAL SOBRE OS DADOS GENÉTICOS HUMANOS, adotada pela Conferência Geral da UNESCO em 16 de outubro de 2003. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/declaracao_inter_dados_genericos.pdf

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS (DUDH). Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/documentos/pdf/declaracao_universal_dos_direitos_do_homem.pdf

DECLARAÇÃO UNIVERSAL SOBRE BIOÉTICA E DIREITOS HUMANOS Disponível em: https://www.ufp.pt/app/uploads/2019/06/declara%C3%A7%C3%A3o-universal-sobre-bio%C3%A9tica-e-direitos-humanos.pdf

DECLARAÇÃO UNIVERSAL SOBRE O GENOMA HUMANO E OS DIREITOS HUMANOS. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/decl-genomadh.pdf

FRANCISCO. Discurso aos participantes no Encontro dos «Minerva Dialogues» (27/III/2023), referido na mensagem do Santo Padre Francisco para a celebração do dia mundial da paz, 1 de janeiro de 2024. Disponível em: https://www.vatican.va/content/francesco/pt/messages/peace/documents/20231208-messaggio-57giornatamondiale-pace2024.html

GRUPO INDEPENDENTE DE PERITOS DE ALTO NÍVEL SOBRE INTELIGÊNCIA ARTIFICIAL, Orientações éticas para uma inteligência artificial, p. 14. Disponível em: file:///E:/Ethics-guidelinesfortrustworthyAI-PTpdf%20(1).pdf.

HOFFMANN-REIM, WOLFGANG. *Teoria Geral do Direito Digital, Transformação Digital Desafios para o Direito, Editora Forense,* Rio de Janeiro, 2021, pp. 11-13.

JORNAL OFICIAL DA UNIÃO EUROPEIA (JOUE)

– Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados): Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679

– Regulamento (ue) 2022/868 do parlamento europeu e do conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento Governação de Dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R0868

– Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos da união. Bruxelas, 21.4.2021. COM(2021) 206 final. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC_1&format=PDF

– Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial (Diretiva Responsabilidade da IA). Bruxelas, 28.9.2022 COM(2022) 496 final. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52022PC0496

MARQUES FILHO, J. Bioética Clínica – Cuidando de Pessoas, Clinical Bioethics – Caring for People in Rev Bras Reumatol, v. 48, n.1, p. 31-33, jan/fev, 2008, p. 32. Disponível em: https://www.scielo.br/j/rbr/a/yfXrdNrjhZpDZsCdNFwgXRw/?format=pdf

MENEZES CORDEIRO. *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019.* Almedina, Coimbra, 2021.p.121.

NAÇÕES UNIDAS. *Interim Report: Governing AI for Humanity, AI* Advisory Body, dezembro 2023. Disponível em: https://www.un.org/ai-advisdory-body

PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 20 de outubro de 2020, sobre os direitos de propriedade intelectual para o desenvolvimento de tecnologias ligadas à inteligência artificial (2020/2015(INI)). Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_PT.html

VITORINO., G; CORDEIRO, J.; MAGALHÃES, T. «A transformação digital nas suas diversas dimensões», in *Transformação digital em Saúde.* Associação Portuguesa de Administradores Hospitalares, editora Almedina, Coimbra (2021).

FICHA TÉCNICA

EDIÇÃO
Câmara Municipal de Lisboa

TÍTULO
Privacidade e Proteção de Dados do Município de Lisboa

COORDENAÇÃO
Cristina Caldeira

AUTORES
A. Barreto Menezes Cordeiro
Alexandre L. Dias Pereira
Alexandre Sousa Pinheiro
Cristina Caldeira
Duarte Rodrigues Nunes
Francisco Rodrigues Rocha
Isabel Celeste M. Fonseca
Joel A. Alves
Jorge Gomes da Silva
Manuel David Masseno
Maria de Medeiros
Maria Helena Silva
Pedro Rebelo Botelho Alfaro Velez
Telma Vitória

REVISÃO DE TEXTO
Jorge Gomes da Silva

DESIGN GRÁFICO
Paula Albuquerque

DESIGN, MONTAGEM, IMPRESSÃO E ACABAMENTO
Imprensa Municipal

TIRAGEM
100 ex.

N.º DE PÁGINAS
324

N.º DE DEPÓSITO LEGAL
528267/24

ANO DE PUBLICAÇÃO
2024

ISBN: 978-989-96864-9-6